Technology Times

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

ims information management systems

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Rick Johnston, Information Management Systems, Fargo, ND

**November 2008
Fargo, ND**

Inside This Issue…

4 ways to protect your computers; don't invite hackers for a Thanksgiving feast
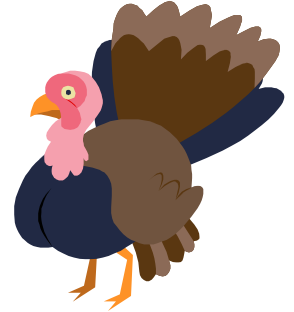
When you step out to partake in the holiday festivities with Thanksgiving just around the corner and Christmas coming soon, do you know your business is protected?

Hackers don't take holidays As a matter of fact, around the holiday season, more malicious websites and e-mails surface than any other time of the year. It is reported that spam messages with links to malicious websites increased 8% within all global e-mail traffic during the third quarter of 2007.

New blended threat techniques now combine spam messages with a link to a website containing malicious software. Watch out! These sites may closely resemble the real deal.

During the kick-off of the National Football League season in September, sports fans became a horrible target for hackers. An infected email went out inviting consumers to download an NFL game-tracker. Talk about a fantastic tool for diligent fans! However, folks were sorely mislead by the quasi-NFL website where all links lead to malware downloads.

Don't take a chance... Here are four basic steps to help you protect your home and work computers from becoming a hacker's Thanksgiving feast:

1. **Use a firewall.** Connecting to the Internet can present dangers to any computer user. A firewall is a software program or piece of hardware that can filter out hackers, viruses and worms that attempt to gain access to your computer over the Internet. A firewall can be put in place at the individual PC level, for laptop or personal use, or on a network as an overall precautionary measure for your business.

2. **Keep your operating system up to date.** No matter what type of operating system you prefer, high priority updates contain the latest protection against malicious online activities. Examples of an operating system update would be a service pack, version upgrade, driver or security update. These critical updates can enhance the security and reliability of your computer improving performance.

3. **Update your antivirus and antispyware software regularly.** Antivirus software is a computer program that can detect, prevent, and disarm or eliminate harmful programs that attempt to compromise your computer and information. Antispyware is roughly the same, but protects you from pop-ups, spyware threats, unwanted software and slow performance. Remember, hackers don't take holidays. So, keep your antivirus and antispyware software up to date in order to help prevent damage from the most current hacker releases. These preventative programs can also be installed on individual work stations or at the server level to protect your entire company.

4. **Use a spam filter.** A spam filter is a software program that blocks unwanted email messages. When purchasing a spam filtering software program, it is important to test the program to make sure it is simple to use and well supported, but still provides a high level of protection to keep you safe.

Protecting your computers internally is a great start to a secure working environment for

If we could shrink the earth's population to a village of precisely 100 people, with all the existing human ratios remaining the same, it would look something like the following:

50 would be female
50 would be male
20 would be children

There would be 80 adults,
14 of whom would be 65 and older

There would be:
61 Asians
12 Europeans
13 Africans
14 people from the Western Hemisphere

There would be:
31 Christians
21 Muslims
14 Hindus
6 Buddhists
1 Jew
11 people who believe in other religions
16 people who are not aligned with a religion

17 would speak Chinese
8 would speak Hindustani
8 would speak English
7 would speak Spanish
4 would speak Arabic
4 would speak Russian
52 would speak other languages

82 would be able to read and write
18 would be illiterate

1 would have a college education
1 would own a computer

75 people would have some supply of food and a place to shelter them from the wind and the rain
25 would not have shelter

1 would be dying of starvation
17 would be undernourished
15 would be overweight

83 would have safe drinking water
17 people would have no clean, safe water to drink

Sources: Fritz Erickson, University of Wisconsin - Green Bay and John A. Vonk, University of Northern Colorado

---

your company. However, many employees and business owners alike fail to consider physical security.

Don't forget to lock your computer when you are away from your desk. To lock your computer quickly use "Windows + L" or the more traditional, "Ctrl + Alt + Del" then choose "Lock Computer" or strike the letter "K".

Strengthen your defenses. Did you know the opportunity for theft or internal compromises increases during the fourth quarter each year? Having a network is just the beginning. Keeping it healthy and safe are the ultimate challenges.

Location and accessibility. If your server is located in a high traffic or highly visible area, it may be easily compromised. Keeping your server in a safe and secure location away from unnecessary exposure can decrease the chances of an internal attack and will discourage burglars in case of a break in.

If you have any questions about the current state of your computers or network, do not hesitate to call us for a **FREE Network Analysis.** We will review each workstation and your server but also look for physical factors that may expose your business to unnecessary harm.

Don't leave your business vulnerable. Otherwise, you may be better off just inviting hackers over for Thanksgiving dinner.

Client Spotlight: Schumacher & Sons

Congratulations to Schumacher & Sons of Grafton, ND on their 75th Anniversary. Four generations of Schumachers have provided outstanding service and quality products to farmers, businesses and residents of NE North Dakota & NW Minnesota. They were one of our first clients when they turned to IMS for their technology needs over 12 years ago. Best Wishes on your significant accomplishment!

Would you like your company highlighted here in our "Client Spotlight?"

Then give us a call today at 701-364-2718

Never Be Lost Again

If you want an easy way to pinpoint a central spot for your next office location or simply view the place you're meeting your next client, you're in luck. Major search engines such as Google (Google Earth), MSN (Virtual Earth) and Amazon (Block View) have rolled out sites that allow you to pinpoint a specific location virtually anywhere on earth.

MSN's site has close-ups that are so clear you can read names on store fronts while Google and Amazon offer services that provide aerial views linked to search engine results so that you get the impression of walking up and down streets.

The photos are not real time but are generally up to date. Best of all access is either low or no cost!

Consultant Update:

Nathan McMillan has recently joined IMS as a consultant. Nathan comes to us from Money Gram in Minneapolis, where he was an Exchange & Security Administrator. Nathan has over 10 years of industry experience. He is a Microsoft Certified Information Technology Professional on Exchange 2007, a graduate of Valley City State University with a B.S in Computer Information Systems and a native of Fordville, ND.

Did You Know These Crazy Facts About

The Search Engine Juggernaut?

Google offers its employees free lunch.

Google's employees get free haircuts.

Google receives more than 1,000 resumes a day.

Over 2.7 billion searches are made on Google search engine each month.

Google can be queried in 36 languages (2007).

Google uses over 10,000 networked computers to crawl the web.

Google, as of 2007, surpassed Microsoft as the world's most-visited site.

The founders of Google didn't know HTML and just wanted a quick interface. That's one of the main reasons why the home page is so bare.

The name "Google" comes from a spelling mistake, the founders intended to write "Googol."

Google launched their search site in 1998.

The Google function "I feel lucky" is nearly never used; well, compared to the high number of users.

Google comes from the word googol, which is 1 followed by a hundred zeros.

Industry feedback on data loss

"93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately."
(Source: National Archives and Records Administration in Washington.)

"Of those companies participating in the 2001 Cost of Downtime Survey, 46% said each hour of downtime would cost their companies up to $50,000, 28 percent said each hour would cost between $51,000 and $250,000, 18 percent said each hour would cost between $251,000 and $1 million, 8 percent said it would cost their companies more than $1million per hour."
(Source: 2001 Cost of Downtime Survey Results, 2001.)

"At what point does loss of data threaten the survival of a business? 40% of companies in the Cost of Downtime Survey said 72 hours, 21% said 48 hours, 15% said 24 hours, 8% said 8 hours, 9% said 4 hours, 3% said 1 hour, 4% said within the hour."
(Source: 2001 Cost of Downtime Survey Results, 2001.)

"Six percent of all PCs will suffer an episode of data loss in any given year. Given the number of PCs used in US businesses in 1998, that translates to approximately 4.6 million data loss episodes."
(The Cost Of Lost Data, David M. Smith)

---

3 Simple - But Critically Important - Things To Protect Your Company's Data

While it's impossible to plan for every potential computer disaster or emergency, there are a few easy and inexpensive measures you can put into place that will help you avoid the vast majority of computer disasters you could experience.

#1: Make Sure You Are Backing Up Your System

It just amazes me how many businesses never back up their computer network. Once it's gone, it's gone permanently!

#2: Perform A Complete Data Restore To Make Sure Your Backups Are Working Properly

Many business owners set up some type of backup system, but then never check to make sure it's working properly. The WORST time to "test" your backup is after a disaster has happened and you desperately need it!

#3: Keep An Offsite Copy Of Your Backups

What happens if a fire or flood destroys your server AND the backup tapes or drive? What happens if your office gets robbed and they take EVERYTHING? Having an off-site backup is simply a smart way to make sure you have multiple, redundant copies of your data!

Give IMS a call at (701) 364-2718 to discuss your Disaster Recovery Plan. For the absolute BEST offsite backup solution, go to:
www.imsnetworking.com/htmls/onlinebackup.htm

Watch your mailbox for our upcoming Total Care Services Program!

Wishful Thinking

A young man said he wanted to be a great writer. When asked to define great, he said he wanted to write stuff that the world would read, that people would react to emotionally, and that would make them scream, cry, and howl in pain and anger.

Ultimately, he got his wish. He works for Microsoft writing error messages.

Greatest Hockey Sign Ever!

Thanks to Keith Gilleshammer of Centre, Inc. for sharing this great sign!

We Want Your Input!

Do you have an idea to make this newsletter better? Would you like to submit a story, article or trivia? We'd love to hear from you!

**Rick Johnston
Information Mgmt. Systems
(701) 364-2718
RJohnston@imsnetworking.com
www.imsnetworking.com**

Harvest your inner password generator

Are you a sticky note password saver? Or avid password recycler? I won't tell, but you may be giving away access to more than your work information if you use the same passwords for personal accounts. Try the CAN password process.

Just remember, use Character, Alpha and Numeric (CAN) values in every password. A survey by Symantec shows that over 60% of us use the same passwords for everything and almost 4% of all users use a single common word found in a dictionary. These habits are very dangerous and can leave you vulnerable to attack.

Here are a few things that are commonly used and easily guessed by intruders:

- Administration - any form of this word.
- Password or Password1 - trivially guessed.
- P@$$W0rd - simple letter substitutions are actually pre-programmed into cracking tools.
- 11/01/08 - avoid dates especially of importance that you have written in an email.
- December03 - avoid using the date of a forced password change, this is also very common.
- nbusr123 - initials followed by "user" or "usr" and a sequence of numbers.
- asdf or qwerty - while these are great memory devices for typing class any sequence of letters or numbers adjacent on a key board are simply out of the question.
- aaaa or bbbb - yyyy not? Repeated letters can be guessed and easily observed by onlookers leaving you completely unprotected.

Please Welcome Our Newest Clients And Friends!

IMS is thrilled to welcome our newest clients to our company! We want to extend a sincere "thanks" for the trust and confidence these clients have shown in us:

**Roers' Construction, Inc.   Roers' Development, Inc.
Professional Property Management   Keller-Williams Roers' Realty**

Don't suffer expensive losses from fraud simply because your password was too weak and vulnerable. Protect yourself with a CAN do attitude and create strong passwords off the top of your head.

Intimidated? Don't be. It is easier than you may think. Character, Alpha and Numeric (CAN) created passwords that are long and random to others but don't have to be difficult to remember.

Create your own personal mnemonic phrases to help you generate seemingly random passwords that others will never guess. For example:

1. IhlesIw4yo! = I have loved elephants since I was 4 years old!
2. K&Igmwiwj22. = Kevin & I got married when I was just 22.

Good luck and remember you CAN create strong passwords just like a password generator.

SHORTCUT CORNER

Key to Press	Action
F1:	Invoke help system or Office Assistant
Shift+F1:	Context-sensitive help or reveal formatting
Alt+F1:	Next field
Shift+Alt+F1:	Previous field
Ctrl+Alt+F1:	Display Microsoft System Information

Watch your mailbox for our upcoming Total Care Services Program!