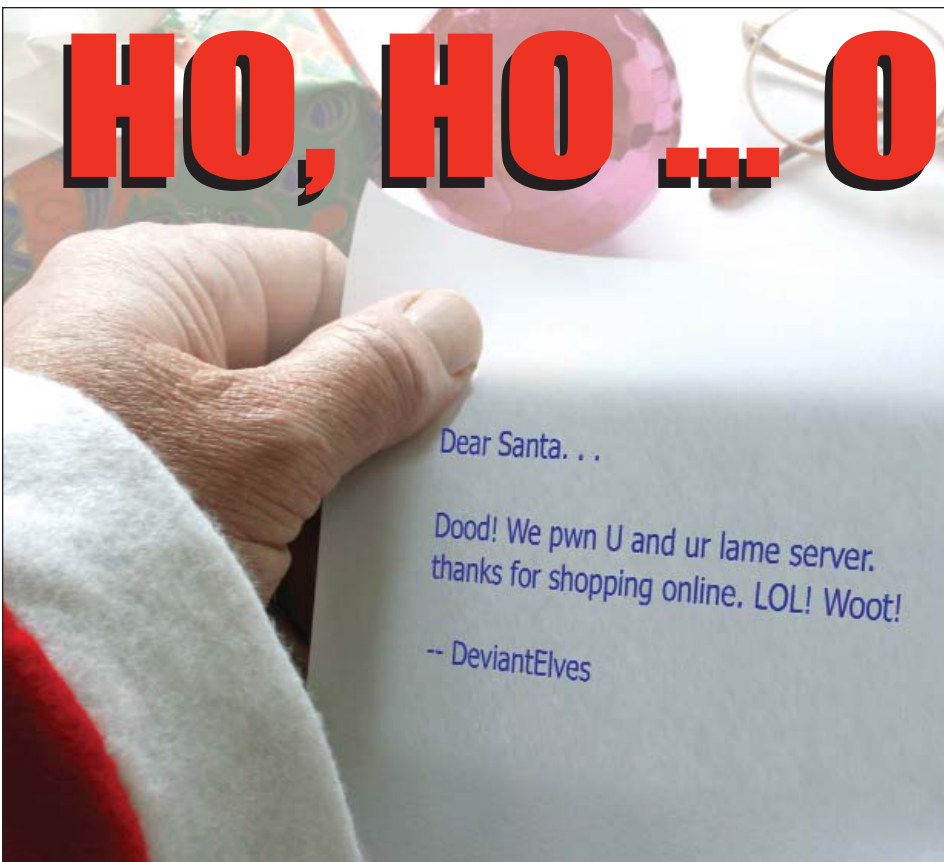


St. Louis Technology News

THE TECHNOLOGY SPIRIT OF ST. LOUIS™

TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH



HO, HO ... OH, NO!

Online shopping plus lack of security awareness make the workplace more vulnerable to spam and viruses during the holidays.

The World Wide Web has become as much a part of the holidays as turkey and mistletoe. Unfortunately, Internet security risks can make the season much less bright for consumers and their employers. Spam, malware and other threats tend to spike during the holidays as cybercriminals try to take advantage of consumers who go online to shop. When employees do their online shopping at work, business systems and networks become more vulnerable to attack unless steps are taken to mitigate these risks.

Online shopping at work has become commonplace according to the recent "Shopping on the Job: Online Holiday Shopping and Workplace Internet Safety" survey conducted on behalf of ISACA, a global, nonprofit associa-

continued on page 2

St. Louis Technology News

PRRST STD
 U.S. POSTAGE
 PAID
 Tulsa, OK
 Permit No. 2146

Ho, Ho ... Oh, No!

continued from p. 1 ...

tion of IT professionals. The survey examined how much time employees will spend in November and December shopping online from work, how aware they are of online security, and whether they comply with employer policies for online shopping. It is based on online polling of 973 consumers in late September 2008 and 3,191 IT professionals in October 2008.

Four out of 10 Americans ages 18 to 24 will spend up to five hours shopping online using their work computer this holiday season. This same age group is the least worried about the vulnerability of their work computers, creating an increased risk of spam, viruses and phishing attacks in the workplace.

Buy Now, Pay Later

Overall, 63 percent of people of all ages surveyed plan to shop online during the holiday season from their workplace computers. However, older Americans are less likely to shop from work than those in the 18 to 24 group, who make up the majority of "Millennials" — a demographic typically described as being more tech-savvy, more concerned about work/life balance and less loyal to their employers than other age groups.

Millennials were also found to worry less about the vulnerability of their work computer than their personal computer. Close to half (49 percent) pay more attention to the security of their home computer than their work computer, whereas almost two-thirds of workers over age 25 are equally concerned with both.

"This survey clearly shows that younger employees are more likely to engage in online activities at work that put a business's IT infrastructure at risk," said Kent Anderson of ISACA's Security Management Committee. "The fact that Millennials are planning to spend the equivalent of more than half a work day doing holiday shopping from their work

computer, combined with their lack of concern for how secure their computer is, points to an urgent need for employee education."

Anderson added that the key is to educate people of all ages on why they need to care about security in addition to how they should ensure their transactions are secure.

Holiday Shopping Bill: \$3,000

Providing a workplace e-mail address to an online retailer can leave a computer network open to a variety of threats and productivity wasters including spam, phishing attacks and viruses. Yet more than two in 10 (22 percent) respondents have clicked on an e-mail link to go to a retailer's Web site from their workplace computer and used their company e-mail address as the contact for a purchase. In addition, one in four (26 percent) respondents either does not check or is unsure how to check the security of a Web site before making a purchase.

These findings are reflected in a parallel version of the survey that was administered to IT professionals who are members of ISACA. According to responses, nearly half (46 percent) believe their company is losing an average of \$3,000 or more in productivity per employee from online holiday shopping at work. More than half (55 percent) also reported that their company permits workers to shop online but has no strategy for educating them about the risks.

"With the economy in such a volatile state, people are working long hours and are facing increased pressure to succeed," said John Pironti of ISACA's Education Board. "The survey results show that there needs to be a common-sense balance between security awareness and employee compliance."

Safer Shopping Tips

ISACA recommends that employees and IT departments take the following steps to reduce the risk of spam, viruses and inadvertent downloading of backdoor "agents" that can highjack corporate data.

For online shoppers:

1. Make sure Web sites you connect to are using SSL encryption while you are entering personal information.
2. Do not allow sites to save your username or password. Avoid providing your work e-mail address as your contact information.
3. Delete cookies from your computer after you are finished shopping.
4. Use separate browser sessions for your holiday shopping versus your work-related browsing.
5. If it looks too good to be true, it probably is. Do not download free games, ringtones, wallpapers or animations onto your work computer.

For the IT department:

1. Train employees on safe computing just prior to the holiday shopping season and follow up with periodic reminders.
2. Tailor education programs to match the various demographics, attitudes and technology know-how of groups within the workplace.
3. Conduct formal risk and threat assessments and update your Acceptable Use Policy and security measures appropriately.
4. Make sure that patches are deployed, security functions are enabled, and firewall rules, intrusion detection system (IDS) signatures, and spam filters are updated regularly.
5. Monitor networks for high-volume or suspicious traffic and respond immediately to threats. Remind employees to sound the alarm if suspicious events occur.

Energy-Conscious Businesses Turning to Virtualization

More and more organizations are turning to virtualization technologies in an effort to improve energy conservation and control power consumption costs, and they are encountering unique challenges in the process according to a recent survey conducted for IT operations management solutions provider Avocent.

A majority of the 299 U.S. executives and IT managers surveyed said that energy conservation and the cost of power were the most difficult issues to resolve with their current tools, and many of the respondents noted that their interest and work with virtualization technology is influenced by the hope of ultimate energy savings.

"The findings further tell us that many administrators lack the tools they need to properly manage power usage in data centers — only 55 percent say they can monitor power usage today, and even then it's mostly at the UPS level," said Ben Grimes, Avocent CTO. "These statistics show there's a huge opportunity to improve overall data center management and a strong desire to implement 'Green IT' solutions."

While a majority of respondents have rolled out some level of server virtualization in an effort to produce cost reductions and energy savings, 24 percent said they have experienced a disappearance of a virtual server from their system and 18 percent said they have permanently lost a virtual server.

St. Louis Technology News

Copyright © 2008 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave., Tulsa, OK 74145

Phone (800) 726-7667 • Fax (918)

270-7134

Change of Address:


Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

St. Louis Technology News is published by CMS

Special Interest Publications. Printed in the U.S.A.

Product names may be trademarks of their respective companies.



Your Behind-the-Scenes IT Team

UltraTech Remote Support is like having a team of highly qualified computer technicians in your small business or home office. Simply call us whenever you have a problem or question, and our techs — with your permission — can remotely troubleshoot your computer.

- ❖ Our techs only gain access to your computer through a one-time-use, six-digit PIN.
- ❖ You watch everything we do on your PC, and can cancel the session at any time.
- ❖ Problems are resolved quickly and cost-effectively, by people you trust.

UltraTech Remote Support. Secure. Fast. Convenient.

UltraTech resources

UltraTech Resources, Inc.
16401 Swingley Ridge Road, Suite 250
Chesterfield, MO 63017
636.594.2004 - Chesterfield
636.978.3200 - O'Fallon, MO
314.985.5646 - St. Louis
877.235.7698 - Toll Free
636.594.2005 - Fax

Microsoft
GOLD CERTIFIED
Partner

Microsoft.
Small Business
Specialist

Wireless to the Nth Degree

802.11n boosts wireless LAN throughput to at least 100Mbps



In the alphabet soup of wireless networking standards, 802.11n is the latest proposed entry. While current WLANs based upon the 802.11 standard have real throughput in the 20Mbps to 25Mbps range, this new version would increase real WLAN throughput to at least 100Mbps, with theoretical raw data speeds in excess of 500Mbps.

Of course, 802.11g WLANs have rated throughput rates of up to 54Mbps, even though actual throughput is only about half that. The proposed 802.11n standard improves the efficiency of media access control to provide end-users with at least

100Mbps of application-level bandwidth — comparable to the wired LAN technology used in most offices. As a result, 802.11n provides the capacity to run advanced applications such as streaming video and Voice over IP (VoIP).

Finding MIMO

At the heart of 802.11n is a technology called MIMO — short for multiple input, multiple output — that employs multiple antennas and radios to transmit and receive data. Although multiple paths typically degrade radio signals, MIMO uses a technique called spatial multiplexing for simultaneous

transmission. This not only increases bandwidth but provides greater coverage, enabling very high-speed connections over distances of 150 feet or more.

In addition, 802.11n uses more of the wireless spectrum, when available, to enhance performance; while 802.11g uses 22MHz-wide channels, 802.11n supports up to 40MHz-wide channels. It is also designed to resist interference from neighboring Wi-Fi systems and 2.4GHz devices.

Slow Route to Higher Speeds

Development of the 802.11n standard was officially announced by the Institute of Electrical and Electronics Engineers (IEEE) in January 2004. The process has been slow, however, with substantial reworking of the original draft. Draft 5.0 was approved in July 2008 and is expected to be finalized in March 2009.

Nonetheless, the Wi-Fi Alliance started certifying products based on draft 2.0 in mid-2007. To date, the Wi-Fi Alliance has put the Wi-Fi certified seal of approval — indicating validated product interoperability — on 325 products and is seeing strong numbers of 802.11n draft 2.0 products presented for testing.

Wi-Fi users have responded to the widespread availability of Wi-Fi certified 802.11n draft 2.0 products with unprecedented enthusiasm. ABI Research forecasts that, by 2013, more than 90 percent of Wi-Fi products will support 802.11n, underscoring the tremendous benefits of advanced Wi-Fi technology and the importance of interoperability certification in delivering the best user experience.

Wide Range of Products

Wi-Fi certified products span both traditional PC networking gear and consumer electronics. Enterprise network managers can now choose from more than 180 Wi-Fi certified laptops, adapter cards and networking solutions that include 802.11n draft 2.0.

Wi-Fi certified 802.11n draft 2.0 products have been tested for interoperability across vendors, adherence to WPA2 (Wi-Fi Protected Access) security protocols, and backward compatibility with more than 4,500 Wi-Fi certified 802.11 a/b/g products. Products based on the IEEE 802.11n draft 2.0 deliver up to five times the throughput and up to twice the range of those based on previous standards, enabling a wide range of content-rich applications, and delivering those applications over a larger footprint. The certification program also includes WMM (Wi-Fi Multimedia) quality of service, which helps deliver the best user experience with applications such as voice, video and gaming.

With a rapidly increasing number of draft-based products entering the market, the Wi-Fi Alliance began certifying products ahead of the final IEEE 802.11n standard to help ensure interoperability and the best user experience. The Wi-Fi Alliance plans to certify products based on the final version of the 802.11n standard once finalized by the IEEE.



GET A CLUE

With issues regarding electronic discovery becoming a central aspect of civil and domestic litigation, legal and paralegal professionals increasingly require the ability to identify, collect, preserve and examine data found on computer hard drives and digital storage media.

Ispirian's digital forensic investigators can help.

Our focus on the digital forensics discipline gives us the training, litigation support experience, report-writing skills and professional involvement necessary to support the e-discovery process and deliver quality, defensible results.

Ispirian's comprehensive case management solution streamlines communication and provides attorneys and support staff with real-time updates as your cases progress. Using a secure Internet portal, Ispirian investigators and their clients can exchange information, update schedules and view key evidence with 24-hour access to budgets, documents, photos and reports.

When it comes to making sense of digital evidence, it makes sense to call Ispirian Computer Forensics: (800) 301-4294.



Ispirian is a member of the High Technology Crime Investigation Association (HTCIA).



Ispirian Incorporated
Chesterfield, MO 63017
Ph: 636.898.1093
Fax: 636.594.2000

Copyright © 2008, Ispirian Incorporated, USA. All rights reserved.
Ispirian Computer Forensics is a Missouri private investigative agency specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA.



The Virtual Desktop

Desktop virtualization promises to improve PC manageability and flexibility.

Deploying and managing traditional desktops represents one of the most time-consuming and expensive operations supported by IT organizations. According to industry estimates, managing a typical end-user desktop can cost more than \$5,000 a year. Unfortunately, even this high level of investment cannot keep pace with the rapid increase in application conflicts and corruptions that degrade user performance, reduce employee productivity, and increase the risk of data loss and security exposure.

Desktop virtualization helps relieve these headaches by consolidating and centralizing complete desktop environments within the data center. Desktop virtualization solutions transform the entire desktop — including operating system, applications and data — into an image that is stored and executed on a server. End-users can access their virtual desktops using a traditional PC, thin

client or other network-connected device.

The potential benefits of the virtual desktop model are so great that many industry experts believe desktop virtualization will ultimately do much more than server virtualization to improve the management of the IT infrastructure. Analyst firm IDC predicts the total market for virtual desktop infrastructure products and services will exceed \$1 billion by 2011.

“Virtualization on the client is perhaps two years behind (server virtualization), but it is going to be much bigger,” said Gartner Vice President and Distinguished Analyst Thomas Bittman. “On the PC, it is about isolation and creating a managed environment that the user can’t touch. This will help change the paradigm of desktop computer management in organizations. It will make the trend towards employee-owned notebooks more manageable, flexible and secure.”

A Better Approach

A virtual desktop functions as though it were running directly on the user's computer, but critical data is kept in the data center where it can be more easily managed and secured. That approach is similar to the server-based computing model, in which servers run the applications and give users remote access via a stripped-down PC or thin client. However, desktop virtualization offers a much higher degree of customization. In essence, servers host an entire desktop environment specific to each user.

Virtual machine images are built and stored on servers and delivered to end-users as needed over the network or the Internet. These images can be customized with the operating system, applications, security settings and other personalization features required by specific users.

Hypervisor technology provides a bridge allowing users to access their desktop environments from traditional PCs or thin clients. When users authenticate to a server, the virtual desktop image gets loaded and boots with all of the preferences set. When they log off, any changes are loaded back into their base virtual image. With these virtual images stored in a central server, users have the ability to access their personalized computing environments from any device and any location, as long as they have a way of connecting to that central source.

Cost Savings, Security and More

Desktop virtualization offers a compelling alternative to traditional desktop management processes. With the ability to provision PCs and other client devices with software from a central location, IT staff can set up new users, workgroups or departments in just minutes, and manage and support a large number of workstations from the data center rather than at each user's desk.

The ability to control and manage desktops and updates centrally reduces the costs normally associated with the traditional distributed desktop model and increases IT efficiency. Workers also become more productive because they can get their full PC experience from any location.

Virtual machines are inherently more secure because operating systems and applications can be updated instantly from the data center. What's more, virtual machines are protected from disaster, disruption, attack and theft.

Traditional distributed desktop computing — where everyone in an organization has his or her own PC or laptop loaded with applications and data — is expensive, complex, time-consuming and insecure. By extending the virtualization concept to the desktop, IT administrators can deploy virtual machines on every PC and deliver a complete desktop experience that is easy to manage, fast to deploy, less costly to maintain, always current and better protected.

all your technology needs under one umbrella



IT staffing solutions? **Check.**

Custom software and Web development? **Check.**

Comprehensive networking and security services? **Check.**

Unlike many other consulting firms, SyllogisTekS has developed unmatched expertise in several critical areas, which allows us to serve as a central source for a broad range of high-quality solutions to complex IT issues.

Contact us today and let us show you how we can help you simplify your business with technology.



Chesterfield, Missouri 63017

Phone: (636) 736.2100 ■ Fax: (636) 736.2101

where are the holes in your security?

According to Gartner, 40 percent of small and mid-sized businesses that manage their own security and use the Internet for more than email will be successfully attacked — and more than half of them will never even know it. Why? Because hackers know that effective security can be too costly and time consuming for most small businesses to implement successfully.

That's why UltraTech Resources has developed UltraShield™, a managed security offering that helps ensure your critical systems and data are protected. UltraShield combines a state-of-the-art security appliance with focused monitoring and management at a reasonable price to provide a solid line of defense against threats ranging from hacking attempts and denial of service attacks to phishing and viruses.

To learn more about UltraShield, contact an UltraTech representative today at 877.235.7698



UltraTech Resources, Inc.
16401 Swingley Ridge
Road, Suite 250
Chesterfield, MO 63017
877.235.7698