Innovations

March fun!

We have a full month this March. We start the festivities off with St. Patrick's Day on the 17th. Don't forget to wear green!

The first day of spring is the following Thursday, March 20th and the very next day is Good Friday, March 21st.

Then, pick up your favorite egg coloring kit and dive into Easter on Sunday, March 23.

By the time you polish off the last of your marshmallow peeps from Easter, it will be time to plan your favorite pranks for April Fools Day, Tuesday, April 1, 2008.

So, pinch your co-workers, eat lots of chocolate bunnies and pull that long overdue prank on your boss.

Have a little March fun!

Tips to avoid getting an avalanche of spam

As you probably already know from first hand experience, once you're on a spammer's list, it's next to impossible to get off. And changing your e-mail address can be a major inconvenience especially if you rely on it to stay in touch with important business and personal contacts.

Reduce the chances of your e-mail address becoming flagged as spam. Once your address makes it on a black list, it is very difficult to work around. These five simple preventative measures that will go a long way in keeping not-so-delicious spam out of your in-box and protecting your e-mail address.

1. Use a disposable e-mail address.

If you buy products online or occasionally subscribe to web sites that interest you, chances are you're going to receive spam.

To avoid your main e-mail address from ending up on their broadcast list, set up a free Internet e-mail address with Hotmail, Yahoo or Google and use it when buying or opting in for online newsletters or promotions.

2. Pay attention to check boxes.

Whenever you subscribe to a web site or make a purchase online, be very watchful of small, pre-checked boxes that say, "Yes! I want to receive offers from third party companies."

If you do not un-check the box to opt-out, your e-mail address can (and will) be sold to every online advertiser willing to pay for a list. To avoid this from happening, simply take a closer look at every online form you fill out even if you use an auto-fill program.

3. Don't use your main e-mail address on your web site, web forums, or newsgroups.

Spammers have special programs that can glean e-mail addresses from web sites without your permission. If you are posting to a web forum or newsgroup, use your disposable e-mail address instead of your business or personal e-mail address.

7 tips for working securely from wireless hotspots

Wireless hotspots are changing the way people work. These wireless local area networks (WLANs) provide high speed Internet access in public locations—as well as at home—and require nothing more than a notebook PC with a wireless card.

From coffee shops to restaurants, airports to hotel lobbies, hotspots are ubiquitous. They are the de facto connection method for travelers and remote workers to access the Internet, their e-mail, and even their corporate networks.

Hotspots range from paid services, such as T-Mobile or Boingo, to free connections at your local coffee shop or library. But they all have one thing in com-

mon: These are all open networks that are vulnerable to security breaches. And that means it's up to you to protect the data on your PC. Here are a few tips to make working in public locations more secure.

1. Try to choose more secure connections.

It's not always possible to choose your connection type—but when you can, opt for wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, which can help protect your computer from unauthorized access. The security

Easter Greetings
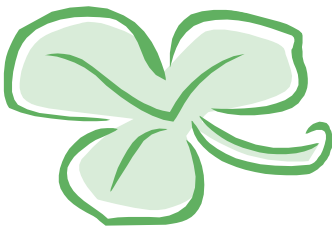
I|T|S
INTELLIGENT TECHNICAL SOLUTIONS

Tips to avoid an avalanche...

(Continued from page 1)
If you want to post an e-mail address on your home page, use "info@" and have all replies forwarded to a folder in your in-box that won't interfere with your primary address.

4. Create throw away e-mail accounts to avoid clutter.
If you own a web domain, all mail going to an address at your domain is probably set up to come directly to you by default. For example, an e-mail addressed to anything@yourdomain.com will be delivered to your in-box. But don't worry, this is a great way to fight spam without missing out on important e-mails you want to get.

The next time you sign up for a newsletter, use the title of the web site in your e-mail address. For example, if the website is titled "business123.com", enter "business123@success.com" as your e-mail address.

If you get an e-mail that look like it could be spam, look at what address the e-mail was sent to and you can easily decipher the senders intentions.

If business123@success.com shows up as the original recipient, you know the source since that e-mail address was unique to that web site. Now you can easily stop the spam by making any e-mail sent to that address bounce back to the sender.

5. Don't open, reply to or try to opt-out of obvious spam e-mails.
Opening, replying to, or even clicking a bogus "opt-out" link in an obvious spam e-mail signals that your e-mail address is active, and more spam will follow.

The only time it is safe to click on the opt-out link or reply to the e-mail is when the message was sent from a company you know or do business with (for example, a company that you purchase from or a newsletter you subscribed to).

If you're getting a ton of spam messages in your e-mail inbox, consider talking with us about our IT Protectorate plans with ITS Antispam services. ITS Antispam offers a great spam and virus filtering system that can help you avoid an avalanche.

Unleash your holiday photos in an instant

Enjoy the ease of instant photo downloads and uploads in seconds. Don't waste another moment looking for your USB cable, you don't need it any more!

Have you ever had a wonderful conversation with a friend or family member that ends in, "I will have to download the pictures and e-mail them to you." With the new Eye-Fi Card you can take all the pictures you want and access them immediately.

Get rid of USB cables.
If you don't mind spending $20-$40 on an extra gadget, the Eye-Fi card can be really handy. It is a storage card that holds pictures and transfers them via Wi-Fi to a preconfigured location. You choose where they go, your personal computer or an online service.

Eye-Fi Card sends photos to websites for you.
You can automatically send your photos to your favorite participating website too. Photo printing companies like Costco.com or Kodak Gallery will accept your uploads and hold them until you are ready to order prints or other products.

If you prefer, keep a gallery of photos on your Facebook page or share web albums through sites like Picasa, Phanfare, or Webshots — it is your choice!

If you're looking for a new camera, keep an eye out for compatible models. The new Nikon D60 is fully compatible with Eye-Fi and offers a variety of storage options. It is a great feature filled compact camera for devoted digital photographers.

Comic company combinations

- If there was a merger between Yahoo and Netscape, the new name might be Net'n'yahoo.

- If there were a merger in the works involving Polygram Records, Warner Brothers, and Keebler. It could be called: Poly-Warner-Cracker.

- 3M & Goodyear would make a delicious company called: MMGood.

- Good advice: John Deere & Abitibi-Price could join forces and become... Deere Abi.

- What could Zippo Manufacturing, Audi, Dofasco, & Dakota Mining be called in the music business? Zip Audi Do Da

- If Honeywell and Imasco join forces with Home Oil, a new name could be... Honey, I'm Home

- Denison Mines, Alliance & Metal Mining = Mine, All Mine

Who wants free movie tickets!

We've added a lot of new customers in the past year thanks to customer word of mouth, and we're looking to grow even more!

If you know someone who needs computer services for their company, we would sincerely appreciate your referrals. You'll get a night out and the person you refer will receive a Free Network Audit to check for viruses and prevent potential problems from creeping up on them.

If your referral turns into a customer for Intelligent Technical Solutions, we will send you a Movie Night for two package. The gift pack includes two tickets to the movie of your choice and a gift certificate good for drinks, popcorn, and candy at the concession stand.

It's our way of saying "thanks for thinking of us." Have a great time!

7 tips for working securely...

features of different networks appear along with the network name as your PC discovers them.

2. Make sure your firewall is activated.
A firewall helps protect your mobile PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks all incoming information, and then either blocks the information or allows it to come through. Microsoft XP or newer Windows operating systems come with a firewall, just make sure it's turned on.

3. Monitor your access points.
Chances are, there are multiple wireless networks anywhere you're trying to connect. These connections are all access points, because they link into the wired system that gives you Internet access. So how do you make sure you're connecting to the right one? Simple—by configuring your PC to let you approve access points before you connect.

Windows Vista takes the guesswork out of connecting to hotspots because you are automatically prompted to approve new connections. In addition, after you approve a connection, you assign it a profile for future use.

4. Disable file and printer sharing:
File and printer sharing is a feature that enables other computers on a network to access resources on your computer. When using your mobile PC in a hotspot, it's best to disable file and printer sharing because when enabled, it leaves your computer vulnerable to hackers.

Remember, though, to turn this feature back on when you return to the office.

5. Make your folders private.
When the folders on your mobile PC are private, it's more difficult for hackers to access your files.

6. Encrypt your files.
You can protect your files further by encrypting them, which requires a password to open or modify them. Because you must perform this procedure on one file at a time, consider password-protecting only the files that you plan to use while working in a public place.

7. Consider completely removing sensitive data from your notebook PC.
If you're working with extremely sensitive data, it might be worth taking it off your notebook PC altogether. Instead, keep it behind the corporate firewall and use your company's VPN to access it when necessary. This way, you have multiple safeguards in place.

A few simple precautions can help make working in public places more secure. And by selecting the best connections and adjusting settings, you can enjoy productive and safe work sessions no matter where you are.

Reprinted courtesy of Microsoft Corporation

"The new diet not working out too good, huh, Frank?"

I|T|S
INTELLIGENT TECHNICAL SOLUTIONS

March 2008

7500 W. Lake Mead Blvd.
Suite 9-196
Las Vegas, NV 89128

(702) 869-3636
(888) 969-3636 toll free

Corey Tom Jeff Kelly

Ryan Sarah Tony

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Ask us about our fixed price service agreements — UNLIMITED support at a flat monthly fee you can budget for just like rent!

News you can use...

Technology spending in 2008 Two factors might make or break the 2008 economy, experts say, and they are old economic friends.

The key factors are consumer spending and strong earnings in big economic sectors like health care, telecommunications, and information technology, according to The Wall Street Journal analysts. Because consumer spending accounts for more than two-thirds of the U.S. economy, any slowdown is cause for worry. At the beginning of 2008 there were lagging sales at companies that provide items that people want but don't actually need. They include expensive dinners, sports tickets and SUVs. The sales lag caused a dip in the stock market, but sales did not totally drop off, as some investors feared.

At the same time, turmoil in the housing and financial sectors led many people to wonder if there would be a recession. But early in the first quarter of 2008, the problem had not spilled over into other sectors. Telecommunications, health care, and information technology all boasted big gains. The Standard & Poor's measure of the operating earnings (down 7.7 percent) would be up about 11 percent if you take off housing and financials.

More online payment options E-tailers are responding to identity theft fears by offering new ways to pay for online purchases.

Google Checkout and PayPal Express Checkout let customers sign up and provide financial details only to them rather than giving credit card numbers to vendors when completing an order.

Another option is Bill Me Later. This payment type sends customers a monthly bill and allows them pay by check through the mail. Verified by Visa and MasterCard Secure Code lets cardholders create passwords that add additional security to their credit card numbers.

Unfortunately, many small and midsize retailers don't offer these new services yet. However, over the next five years, many companies will adopt these new security features to ensure customers feel at ease shopping at their online stores.

Protect your digitals Laptops, cameras and music players are take-along equipment, which means they could be lost or stolen. Check with your homeowners insurance agent to see if your gear is covered. A simple task of recording the serial numbers so your camera or computer can be identified after a theft can save you quite a headache. Police can check the numbers against recovered property to find your missing items. Your insurance company might also need them to process an accurate claim.

Don't Rely On Luck!

Imagine if you lost days worth of work, financial records, or even your entire client database. What would happen if your network went down and no one could access e-mail or files. How frustrating would that be?

Give us a call today to set up your Free Network Audit. We will identify potential threats to your network and help you prevent down time.

Intelligent Technical Solutions
(888) 969-3636
help@itsasap.com
http://www.itsasap.com