

Storm Season is Just Around the Corner...	2
People Tell More Lies	2
Hidden Web Site Reports	3
Important Email Etiquette Rules	4

TechTip Newsletter

March/April , 2009 Volume 4, Issue 2

How To Keep Your Laptop Secure When Using Public Wi-Fi Hotspots

They're everywhere these days. Wi-Fi hotspots for checking e-mail and hopping on the Internet can be found in airports, coffee shops, book-stores, and even most fast food joints—there's even one in the Stop and Shop Supermarket in Plymouth. For the uninitiated, Wi-Fi hotspots are areas where you can use your wireless laptop to surf the Web and check e-mail.

But have you ever wondered, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all time high, you are smart to be concerned. Unfortunately, it's easy for a hacker to set up a Wi-Fi hotspot to access your laptop, called an "evil twin." An evil twin is a wireless hot-spot that is used to lure people from a nearby, legitimate hotspot. For example, when logging in at your favorite coffee shop, you may have inadvertently logged into an evil twin Internet connection set up by the person working on a laptop at the next table.

Just like legitimate sites, evil twins allow you access to the Internet, but in the background they're recording everything you type. Log onto your email, investment website, bank account, or buy something online, and they are recording your keystrokes.

You may be asking, "How do I protect myself at Wi-Fi hotspots?" First you need to make sure the hotspot is legitimate. You can do this by asking someone who works at the Wi-Fi location; in fact some businesses will give you printed instructions that include the hotspot name. Even

Tip: Do you want to securely access your network and the Internet from anywhere? Call us today at 781-834-9208 and ask about setting up a VPN connection for your office!

here you need to be careful. Many times, in an attempt to make you feel comfortable, the hacker

will use an evil twin name that mimics the legitimate hotspot and, on some occasions, the fake site may even show up at the top of your network list by having a stronger signal than the legitimate site.

The best protection is to connecting to your company's network via a VPN (virtual private network). A VPN protects you by encrypting your data and activity even if you're connected through an evil twin. If you don't have a VPN connection, it's "fairly" safe to surf the net, but never type in passwords, credit card, social security, bank account, or other sensitive information when connected to a public Wi-Fi hotspot.

Monday's Marketing Minute



Pam Snell has been marketing for over 35 years (since she was 4??) and is now offer-

ing that knowledge to everyone in her FREE email newsletter "Monday's Marketing Minute"

Let's face it, in this economy we all have to work a little harder and smarter. Every Monday she offers advice and suggestions on how to market your business more effectively. Here's a few of the comments we've received:

Great newsletter! Keep up the good work. ~Dr. S., Duxbury

*I read every word! It's GREAT!
~ Scott Matthews,
Matthews Electric*

If you're not getting your FREE subscription, just go to MondaysMarketingMinute.com or to ACTSmartWeb.com and sign up today.

Take advantage of Pam's many years of experience understanding the difficulties of small business marketing. Your questions and comments are always welcome!



Storm Season Is Just Around the Corner... Are You Protected?

Even though the first day of Spring is not until the 20th of March, it's never too early to prepare for those pop-up storms that occur randomly at this time of year often resulting in everything from ice damage to lightening fires. During this time of year the threat of fire, flood, severe storms, water damage from office sprinklers, and even theft is very real.

One of the most valuable assets for any company is its data. Hardware and software can easily be replaced, but a company's data cannot!

As a reminder to all of our clients, here are some simple things you should do to make sure your company is ready for any natural disaster.

Back Up Your Data Remotely! Everyone knows that data should be backed up on a daily basis, but many people still use in-house tape drives that will get damaged in a natural disaster or fire, and can easily be stolen. We recommend backing up all data to an off-site location, and we offer this as a service to our clients.

Use a Quality Surge Protector With Uninterruptible Power Supply Battery. A high quality surge protector combined with an uninterruptible power supply battery backup will go a long way in protecting sensitive electronic equipment from surges and other electronic irregularities that can destroy your computer's circuitry.

Make Sure Your Servers Are Off The Floor. If your office gets flooded, having your equipment off the floor will prevent it from being completely destroyed. Server racks can be purchased and installed very inexpensively.

Have A Disaster Recovery and Business Continuity Plan. Every business should have some type of plan in place for continued operation after a disaster. Would people know where to go? Who to call? How to log in and access data remotely? Hopefully you'll never need it, but having a simple plan will make you sleep a lot easier at night knowing you have a way to continue to operate when disaster strikes.

If you need help in any of these areas, give us a call! We can not only get you prepared, but also back up and running fast in the event of a disaster.

New Study Reveals People Tell More Lies With E-mail



You might not believe a "get rich quick" offer sent by a stranger, but when a message comes from a friend, you may be more likely to think it is believable.

But don't be TOO sure! Researchers from Rutgers and DePaul Universities found that more people lie in e-mail communications than verbally or in writing. Why? Because there seems to be a "reduced feeling of social obligation" when sending e-mail.

The better you know the recipient, the less inclined you'll be to lie – but many of the people in the study admitted that they still stretch the truth, even with friends and colleagues.

Another study found that people are far more likely to be overly critical in email than on paper. So as the owner of a company, you might consider getting feedback via e-mail to elicit frank responses.



How To Unlock Secrets About Your Customers Hiding In Your Web Site Reports

No matter who hosts your web site, it's almost certain that you have web site traffic reporting. These reports can tell you a LOT about your customers and who is visiting your web site IF you know how to read them. Here's a quick lesson on how to decipher them...

Hits Vs. Unique Visitors

It's been said that "hits" is short for "How Idiots Track Sales." Total Hits is a deceptive number because a single visitor on a single page could easily pull a dozen files (hits) or more.

The number you should watch is "unique visitors" or "unique referrers," the best indicator of how many individual people are actually visiting your site. If your number of unique visitors is extremely low, it's either a sign of weak marketing or a technical issue. Sites built in Flash or that use images instead of text are difficult for search engines to index and, therefore, will get very low rankings and traffic.

Browsers

Your reports should give you a list of web browsers your clients are using when coming to your site. With multiple browsers being used by web surfers, you need to make sure your site works with all the browsers identified in your reports.

Exit Page

If you're not getting web visitors to "convert" by buying, signing up, or doing something else you want them to do, take a closer look. Why are people leaving? There may be a technical issue, a bad headline (or no headline), no offer, slow-loading graphics, or confusing copy. Something on this page is making your visitors leave without doing what you want them to do.

Experiment with various headlines, offers, and designs until you find something more successful.

ACTSmart Tip: Offer a downloadable "white paper". This can be a report that not only shows you as the expert—it can also capture the visitor's email address so you can use it for future targeted marketing!

Update Keywords and Keyword Phrases

Be sure your web site key words line up with the words people use when searching for products or services you offer. Keeping these aligned will allow you to optimize your conversion rate and minimize your expenses when using pay-per-click search engine marketing. Your website designer or web master should be able to provide low cost services to evaluate your keywords.

Errors

Check out the error list from time to time to make sure you aren't experiencing any technical issues. The most frequent error you'll find is a "404" code, which means "document not found"—also known as broken links which occur most frequently with site updates or old external links.

A clever tip is to have a custom "404" page that shows up instead of the stock standard "file not found" page, that contains your company name, phone number, and a way to report the problem. Your web master can set this up for you.

Monitoring and updating your website regularly can be the difference between maintaining a web presence or having a virtual selling machine on the web.

Most of our clients have been switched over to Google Analytics, a FREE statistical report that is inserted into your website. If you don't have Google Analytics, aren't sure how to use it or if you have any statistical questions, give us a call.



"Go ahead and laugh, but this baby hasn't crashed since 1961."

The 23 Most Important Rules Of E-mail Etiquette

More than 80 years have passed since Emily Post wrote her first book on etiquette. Back then, the rules had more to do with how to properly introduce someone and which fork to use at a dinner party. But with the introduction of new communication tools comes new rules of engagement. Here are 23 quick tips and rules for what is—and isn't—acceptable behavior when using e-mail.

1. Be concise and to the point. Read your e-mail to make sure it makes sense before sending to avoid e-mail "ping-pong."
2. Don't reply just to say "got it" unless the recipient has asked you to.
3. Use proper spelling, grammar & punctuation. This is still a communication and a representation of YOU. Sloppy spelling and punctuation looks unprofessional.
4. Don't use e-mail to deliver bad or personal news. If you need to discuss a serious matter with someone, only use e-mail to request a face to face meeting or phone call, not to deliver the news.
5. Do not attach unnecessary files, especially large ones. Sending big files can cause someone's e-mail system to clog, shut down or crash. Instead, use www.yousendit.com for large documents.
6. Do not overuse the high priority option. Use it only when something is truly critical and time sensitive.
7. Do not write in CAPITALS—it's considered the equivalent of shouting.
8. Don't leave out the message thread.
9. Give your recipients an easy way to opt-out or remove themselves from your list.
10. Do not overuse "Reply to All." If you have a message for the sender that is not relevant to everyone else, make sure you only send it to that person.
11. Do not cc everyone when sending a broadcast to multiple people. Instead, use the bcc (blind carbon copy) to keep everyone's e-mail private.
12. Don't overuse abbreviations and emoticons.
13. Don't use neon colors, hard to read fancy fonts and background images. They make it difficult—if not impossible—to read your message.
14. Only use rich text and HTML messages when you are certain the recipient can receive that type of message. Many people can only open text messages, and most rich text and HTML messages don't convert well.
15. Do not forward chain letters, ever.
16. Do not request delivery and read receipts.
17. Do not recall messages.
18. Do not forward a message that was sent to you without permission from the original sender.
19. Do not use email to discuss confidential information. A good rule of thumb is this: if you don't want the entire world to see it, then don't put it in an e-mail.
20. Use a meaningful subject line to help the recipient sort through their inbox.
21. Don't send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. They aren't funny and if sent using company e-mail, they could get you sued or fired.
22. Keep your anti-virus up-to-date to make sure you don't spread viruses to your friends.
23. Don't reply to spam; it only signifies that your address is active to the spammer and will invite more of the same.



I'd Love To Hear From YOU!

Is there an article or feature you would like me to include in this newsletter? DO you just want to "sound off" about something or share your opinion with my other subscribers. Let me know!

769 Plain Street, Unit L, Marshfield, MA. 02050
781-834-9208 or David@GoAmerican.com

www.GoAmerican.com
www.ActSmartWeb.com
www.ActSmartBDR.com
www.IronCladBackup.com