April 2015

TechTidbit.com

brought to you by Tech Experts

Social Media Hashtags: What Are They And How To Use Them?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

As we delve into our social media networks, like Instagram, Twitter, and Tumblr, it seems that hashtags - or little words and phrases preceded by the # symbol - are permeating everything in our feeds.

This cryptic little symbol can actually make it easy to categorize posts and search for similar content, but more and more people seem to be using it outside of that purpose, which creates confusion about this practice as a whole.

Unlike many internet crazes, the emergence of the hashtag can actually be traced to its very first Tweet.

Back in August 2007, Chris Messena, a former Google employee, wrote on Twitter: "how do you feel about using # (pound) for groups. As in #barcamp [msg]?"

Granted, this single tweet didn't revolutionize how we navigate social media all at once, but it eventually did catch on.

When used appropriately, they can gain much exposure for your business or things that interest you most.

You can make up your own hashtag, but you should take care to choose something that clearly states its purpose, so it won't be confused with another brand or topic.

Another option for using hashtags to gain exposure is to proverbially ride on a trending hashtag's coattails.

For example, if your business offers a product or service that is closely related to a popular event, item, or person, using that trending tag will bring up your message in those search results. Also, consider using tracking and analytics, such as what Sprout Social Trends provides, to find hashtags people already associate with your business and use them to your advantage.

Finally, know what social media networks are best adapted to using hashtags. This is one practice where Facebook isn't your go-to place.

While Twitter and Instagram are the hashtag kings, there are scores of other platforms made for this kind of categorization, including, but not limited to, Pinterest, YouTube, Google+, Tumblr, Vine, and Flickr.

Don't be afraid to experiment with this powerful categorization tool. With time, observation, and practice, hashtags will be able draw lots of potential customers you may otherwise miss through conventional advertising to your website or social online business presence.

HIPAA Email Encryption Requirements

Michael Menor is Vice President of Support Services for Tech Experts.

Question: does the Security Rule allow for sending electronic patient health information (e-PHI) in an email or over the Internet?

Answer: the Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected. The HIPAA Security Rule does not expressly prohibit the use of email for sending e-PHI.

However, the standards for access control, integrity, and transmission security require covered entities, such as insurance providers or healthcare providers, to implement policies and procedures.

These policies and procedures restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI.

The standard for transmission security also includes addressable specifications for integrity controls and encryption.

By default, whenever you send or receive email, you must connect through the Internet to an email service provider or email server.

The reality is that most email service providers do not use any security at all. This means everything you send to or receive from your email service provider is unsecure, including your user name, password, email message, attachments, who you are sending to, and who you are receiving from.

It gets worse! Most email service providers connect to other email service providers without any encryption.

If the other party is not using a secure email service, their emails can also be compromised. So the email you send and receive through the Internet is wide open, unsecure, and can be intercepted and stolen by thieves.

This is one of the main causes for identity theft, spam, and PHI breaches.

According to the U.S. Department of Health & Human Services (HHS), "…a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative."

This basically states that encryption is required. If you choose not to encrypt your data, you must document, in writing, a reasonable explanation why you chose not to do so.

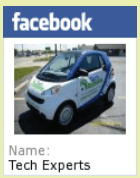
In the event of an audit, the Office for Civil Rights (OCR) will review your documentation and determine whether or not they agree with you. You're required to encrypt PHI in motion and at rest whenever it is "reasonable and appropriate" to do so.

I'll bet that if you do a proper risk analysis, you'll find very few scenarios where it's not. Even if you think you've found one, and then you're beached, you have to convince the OCR, who think encryption is both necessary and easy, that you're correct.

I have convinced myself and others that encryption is required by HIPAA.

Better safe than sorry, after all.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

Top Signs Your Computer May be Infected

Scott Blake is a Senior Network Engineer with Tech Experts.

Ranging from minor spyware and adware to complete system lock-outs courtesy of ransomware, infections have become a standard in today's high-speed electronic age.

Even when using the latest state of the art detection software, the most modern systems are prone to infection.

Some basic low-level forms of adware and spyware are add-ons called toolbars. A toolbar is an add-on to a web browser, putting another bar at the top of your browser window below the address bar.

They can come in several different forms and functions. Some are helpful and pose no threat to your system. Others serve as a reporting tool for the toolbar's designer.

They can collect data on surfing habits such as websites visited and search topics used. This data is then transmitted back to the designer and sold off to advertisers who, in turn, use the information to start spamming you with their client's websites and ads.

Building off of the spam generated from the data collected from the adware and spyware, you will start to see more and more pop-ups on webpages and possibly even on your desktop.

Sometimes, these pop-ups are harmless and very easy to remove, but more often, they are the beginning stages of an invasion of malicious programs.

The pop-ups use false and misleading information to scare the user into believing they are already infected and they need to download "their" software to clean the infections.

What ends up happening is that you think you are downloading one program to clean your system, but you are really downloading and installing additional programs in the background.

I have seen instances where one so-called program install downloaded nine additional programs in the background. None of the additional programs had anything to do with "cleaning" or "speeding" up your system. They just wreak havoc on your operating system.

Through these malicious programs, more dangerous infections can occur. High-risk level malware, trojans, and viruses become residents on your system.

From this point forward, you will start to experience extreme slowness or even a complete inability to browse the Internet. You will start to see an increase in spam email and email messages containing attachments or web links to strange web addresses.

The attachments are what you need to be very cautious about. A very high-risk level malware called Crypto is primarily transmitted through these infected attachments. Once infected, the Malware spreads though your system, encrypting all of your data.

After that, there is little hope of recovering any of your data.

Viruses, malware, trojans and malicious programs are lurking on the web at every turn.

The most important thing to remember is "knowledge is power." Don't fall victim to the overwhelming number of companies advertising that their products can and will clean your computer of these nasty bugs and speed up the performance of your computer at the same time.

The truth is that the vast majority of these companies will install a ton of "freeware" programs on your system that will bog down your CPU and eat up your memory resources.

Once these programs are installed, get ready for Pop-Up City. It turns into a giant game of Whack-A-Mole just trying to close all the windows and pop-ups generated by these programs.

Several of these programs will also inject a proxy server into your Internet settings. This will severely limit your Internet browsing and even redirect you to predefined webpages in an attempt to lure you into purchasing additional programs to remove the programs you already installed.

For additional information or if you think you may have a virus or spyware infection, contact Tech Experts at (734) 457-5000.

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Is Skype For Business Right For Your Company?

Last month, Microsoft released its vision video preview for Skype for Business, which suggested some major changes to ways we currently conduct business.

The video shows a wrist-worn communication device that allows you to contact colleagues on the fly. It also illustrates how Skype can help people be virtually present in the office while actually working in the field.

Skype-powered technology can integrate data into one space and share it on a big screen to facilitate brainstorming, can instantly translate speech into a number of languages, and even simulate a doctor's house call – if what is depicted in the preview becomes a reality.

Really, nothing in Microsoft's Skype for Business preview is all that far-fetched. Skype has already drastically changed how people keep in touch on both business and personal levels.

Presently, you can video chat with anyone, anywhere to conduct interviews or meetings. It's not that big of a leap to envision using Skype to do these same things in the great outdoors or to integrate it with web searches and data files. The basic technology is already there; the vision video just shows some tweaks and new exciting applications.

The possibilities illustrated in the preview video highlight Microsoft's mission to develop cross-platform technology that increases productivity.

While Skype for Business may not initially perform as seamlessly as the video leads us to believe – especially when real-time translation has yet to be perfected – there are products already advertised that do similar things.

Microsoft's Surface Hub combines Skype with an 84-inch touchscreen display, and the HoloLens promises to take holograms and headsets to the next level.

Is Someone Using Your WiFi? Here's How To Find Out

There's no doubt about the convenience of using wireless in your home or office. However, you don't want just anybody hopping on your WiFi, using your network, and breaching its security. Having a unique password doesn't mean you are immune to this problem.

If you ever notice that your connection is much slower than usual, it's worth taking a peek at just how many devices are connected to your wireless network.

You can download and install a program aptly called "Who Is on Your WiFi" to know if there are other people connected to your hot spot who should not be. The free version is sufficient to detect intruders, but there are also paid versions with extra features like text notifications, audit logs, etc.

Once you install the application, all you have to do is follow the tutorial to run a scan of your network and review information about devices that are linked to your connection.

Initially, you may not recognize which MAC and IP addresses correspond with which device, but there's an easy way to identify them. Turn off all of your devices, then turn them on one by one. If you only have one known device connected to your WiFi, and the "Who Is on Your WiFi" application is showing more than that device, it's a safe bet someone is sharing your Internet connection. Take the appropriate measure of immediately changing your wireless password and only share it with family or designated individuals you want to have it.

For future scans, you can label each of your devices as something easily recognizable, such as My Phone or Dad's Laptop, to facilitate the identification of intruders.