Paradigm Computer Consulting

# TechAdvisor Newsletter

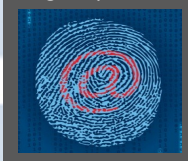
## June 2012

*Your Small Business Technology Information Source!*

## This Issue:



Computer Infected? The FBI is turning off your Internet



Computer viruses are pretty serious threats, and can cause huge expensive issues for businesses. Many cases of malware and computer viruses actually use your computer to commit real crimes. The FBI states that hundreds of thousands of people will likely lose the ability to surf the web.

**Read the rest Online!**
**http://bit.ly/MHbFQm**

## About Paradigm

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
**newsletter.paradigmcomputers.com**

## Is your Business a Victim of Email Spoofing?

Is your email sending out mass-mail spam messages? Have you ever received a complaint about sending unsolicited ads or obvious spam messages? Have you ever received bounced emails by the boatload that look like they have been sent from your own account, even though you know you didn't send them?

If you are in the above situation, it is likely your email is being spoofed. Email spoofing is where spammers try to trick spam filters by making spam look like it comes from a legitimate address. They do this by manipulating the email header to display your email in the "from" address, hence why you get bounces back and others believe the junk mail is coming from you.

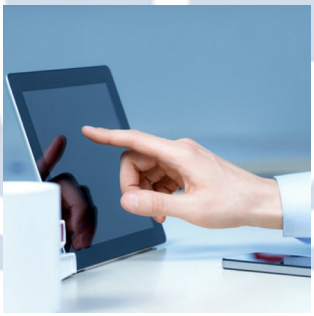
This isn't the same as having your email compromised, which is where spammers can actually get into your email account with your password and create havoc. While it's a good practice to change your email password if you notice something fishy, spoofing doesn't need access to your account to get in. Spammers do this because an email is much more likely to get attention if it's from a recognized sender.

### What To Do To Resolve Email Spoofing

In some cases, an experienced IT technician can investigate the header of the email and determine the true origin. This won't typically catch the spammer, but it will point the technician to the internet service provider. At that point, the next course of action is to reach out to that ISP and have that IP blocked. This doesn't mean you won't be targeted again; the spammer could simply reinitiate the spoofing process from a computer on a different IP, and

*(Continued on page 3)*

## Has Mobility Changed Your Business?



Technology is changing quickly and businesses are seeing a wide variety of options replacing traditional IT methodology that is driving change and productivity to businesses of all sizes. It's getting easier to take work with you with mobile devices and hosted services, but are these just expensive new toys or do they provide serious benefits to businesses?

### Cloud Computing

Probably the biggest, vaguest buzz word of this technology generation, cloud computing can mean a whole lot of different things. From a technical standpoint, one definition of cloud computing is the infrastructure required to split computing power between a mass of devices, although there are publicly available clouds like Google and Amazon, private clouds that larger businesses establish, and even social networks and a slew of various web apps have been considered 'the cloud.'

*(Continued on page 2)*

## Has Mobility Changed Your Business?

*(Continued from page 1)*

Okay, so cloud computing is a big, ambiguous thing. However, leveraging the idea of the cloud offers cost-saving benefits to small businesses. Dropping the semantics, when a company doesn't need to worry about managing a part of their IT infrastructure in house, they save money. It's that simple. Let somebody else take care of it and make sure it works. Sure, there is a cost to this, but without the need for new hardware, space, electricity, heat disbursement, maintenance, and all of the other things that get tacked on with a best-practices server room, eliminating some of the hardware quickly adds up to big savings.

Mobile Devices

About half of all cell phone users own a smart phone. We might not have flying cars yet but we do have access to powerful handheld computing devices that keep us connected to both our personal and professional lives and give us the ability to work seamlessly from anywhere. Partially, mobile computing is related to cloud - the mobile platform is still fairly light weight and requires something else to do the heavy lifting and store the data. Still, businesses will be seeing a shift from traditional chained-down desktops to functional, accessible tablets, laptops, and smartphones, that is, if they haven't already.

> ***"mobile technology increases productivity . . . Users can access files and applications from anywhere. . ."***

The biggest improvement seen by adopting mobile technology is productivity. Users can access files and applications from anywhere, communicate and correspond easily from their mobile device, and stay productive while on the road. For most small businesses, employees might bring their own smartphone, but mobility is not going to be a fad. Business application developers are feeling the push and developing software that plays nice with tablets and smartphones. Eventually, this shift could lead to the eventual death of the desktop workstation as we know it for many types of employees, but harbor new and innovated ways small businesses get things done.

Technology is always changing and can drive businesses forward when adopted carefully - whether you want to save money or improve your bottom line's productivity or just provide better, more accessible options for your employees, Paradigm can partner with your New Hampshire and Massachusetts business and help prepare your company for the technology benefits of tomorrow.

**Share this Article!**
**http://bit.ly/L3xQvO**

## Why Should I Safely Remove Devices?

If you've used a USB flash drive or other USB devices like cameras, smartphones, and external hard drives, you've probably seen Windows request you to safely remove the device as opposed to simply unplugging it from the PC when you are done. How important is this? Very.

Think of a passenger jet being loaded with luggage - if the captain starts to taxi the plane before the cargo is loaded there is going to be a problem as some luggage will get lost or damaged. The same can happen with the data on the USB device; abruptly unplugging it while data is being read or written can cause it to be lost or damaged.

Even if you know you aren't copying files from your digital camera or thumb drive, a program could still be operating behind the scenes and using the device.

To disconnect devices correctly, look on the bottom right of your screen in the system tray. You may have to click the arrow to expand and display all icons. Right clicking on the icon will display a menu with the option to Eject USB Mass Storage Device. Click that, and your PC will properly prepare the device for removal. It typically only takes a couple seconds.

If you can't find your device or aren't sure which one to select from the menu, there is an even easier way. Go to My Computer, you should see an icon for your device. Right click on that and select Eject.

Windows will let you know that your device is now safe to remove, and then you can do so.

Is your business running with the best IT practices to ensure the longevity and continuity of your IT investments? Contact Paradigm at 603-647-8614 and ask us about ways to improve your day-to-day operations through better use of your technology.

**Share this Article!**
**bit.ly/MH638J**

## Is your Business a Victim of Email Spoofing?

*(Continued from page 1)*

you'd need to hunt them down all over again.

### Prevention Goes a Long Way

It's very difficult to stop spoofing attacks permanently - businesses need to take action to prevent them. Be aware of phishing attacks (spam emails that link to fake pages meant to look like legitimate website login pages) and ensure you are keeping your anti-malware and antivirus software up-to-date. Unfortunately, it actually doesn't take any negligence to open yourself up to email spoofing, spammers just need to know your email address.

Using throwaway email addresses for signing up for accounts is a good way to keep this in check. Use your main email only for correspondence with people, and have a couple email accounts specifically for different accounts on the web. For example, setting up a social@ email for social networks like Facebook and Twitter, or create throwaway accounts for signing up for sites that you don't completely trust. It isn't to say that the websites you sign up for are spoofing your email, but if hackers gain access to your login data for that site, or if the site shares your personal information, it's possible your email could get into the wrong hands.

If you suspect that your email is compromised or spamming others, contact us at Paradigm at 603-647-8614.

**Share this Article!**
**http://bit.ly/L3wNw0**

## Take Back your Bandwidth

"Almost 40% of enterprise network bandwidth is being consumed by recreational or non-business applications [facebook, linkedin, youtube]"
~Blue Coat Systems Survey

More companies are blocking video streaming sites such as YouTube and Netflix to improve productivity at work.

USA Today mentions that Proctor & Gamble "Has shut down access to Pandora and Netflix for its 129,000 employees" Leaving sites such as Youtube and Facebook available since they are required for business. As more and more people have tablets and other mobile devices , the use of recreational internet usage stands to rise. Web apps and streaming services eat up a lot of bandwidth, sending large audio and video files, most of which are completely unrelated to work, and worst of all greatly stagger productivity.

Not all web content is bad for business, however. Social media has profoundly potent marketing benefits for businesses and completely blocking sites like Twitter and Facebook can put a hamper on inbound marketing tactics for your sales and marketing people. Having precise control to offer certain users specific access will help you take advantages of the benefits and plug up the time leaks.

So what can your business do about it? Implementing a content filter/firewall solution on your network can give you precise control over who can view what content on the web. This will let you block sites like Facebook and YouTube for your general staff but leave them open for your marketing department to allow them . . .

**Read the rest Online!**
**http://bit.ly/MH6ZKf**

## Disabling Those Pesky Browser Toolbars

Browser toolbars: some people love them, some people hate them, others just don't care. Browser toolbars can make surfing the web easier, but sometimes they can get in the way and slow things down, and even open you up for potential risks.
First, what are toolbars? Toolbars are add-ons that can be downloaded and integrated into the top of your browser window. They add in extra functionality and shortcuts which can make your browsing experience more enjoyable. Many toolbars provide one click access to your email, or your favorite websites. Others, like the Yahoo toolbar can provide added security and still others, like StumbleUpon are just for fun. Typically you install toolbars from their related website, however sometimes software installations will sneak a toolbar in that you didn't want.

There are many drawbacks to having multiple toolbars. The most obvious downside is real estate: the more rows of icons, links, and search fields you have on your browser the less visible space you have available for the websites you visit. Toolbars can increase the time it takes to load web pages. The really bad

*(Continued on page 4)*

Paradigm
Computer Consulting



## Disabling Those Pesky Browser Toolbars

*(Continued from page 3)*
toolbars will hijack your browser and force you to websites you didn't want to visit. Removing unnecessary toolbars is a good practice from time to time because by doing so, you can unclutter your screen, improve your browsing speed and cut out security risks that may be associated with them.

To remove a toolbar in Internet Explorer, all you need to do is click the tools menu on the top of the screen and choose Manage Add-ons (you may need to activate the menu bar, by right clicking the very top part of the browser window and left clicking Menu Bar). From the Manage Add-ons window make sure that Toolbars and Extensions is highlighted, then you simply choose the toolbar you want to get rid of and click disable. It may tell you that other add-ons will need to be disabled in order to finish the process, click ok. Once that is all said and done, you can click close.

In Firefox, the process is almost identical. Click tools, then Add-ons and a page will open in a new tab. From here, click Extensions on the left side, and choose the toolbar or extension you want, then click disable.

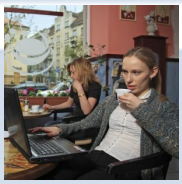
While there are some benefits to having toolbars, there are drawbacks which may outweigh those benefits. If for some reason the toolbar keeps coming back, just give us a call at 603-647-8614 and have one of our technicians check out your PC. You likely have some malware that is trying to take over your browser.

**Share this Article!**
**bit.ly/MH8Gr4**

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Shawn Walsh
CEO

## Public Safety Tip: Wi-Fi Hotspot Security



When traveling with your trusty laptop or tablet, it's pretty common to find publicly accessible Wi-Fi networks that you can connect to, enabling you to surf the web. Where ever you are, whether it's a coffee shop, hotel, airport, or anywhere else, it's important to be safe about public surfing.

There are some risks involved when connecting to public networks, mostly because you don't know who or what else is on the network. Following a few simple tips can ensure that your mobile device and data remain safe.

**Only connect to secure hotspots**
This will greatly limit your ability to connect to the Internet at public locations, but it removes a whole lot of risks. Many places that offer free Wi-Fi password protect the network. This controls who is on it and encrypts the data being sent across the network. Otherwise, you open your device up to the entire network and all the risks associated with it.

**Read the rest Online!**
**bit.ly/MHa0ue**

Tom E. Mitchell
COO

**Paradigm Computer Consulting**

2 Townsend W Ste 3
Nashua, NH 03063-1277
603-647-8614

facebook.paradigm.com
linkedin.paradigm.com
twitter.paradigm.com
blog.paradigm.com
newsletter@paradigm.com

Visit us **online** at:
**newsletter.paradigmcomputer.com**