

TechTidbit.com

brought to you by Tech Experts

Staying Connected When You Travel



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

some tips to stay in touch and connected - but only if you want to!

Cellular and mobile broadband

The single biggest change in mobile technology is the ubiquity of relatively high speed data service. Coverage has increased significantly, and speeds rival that of low-end landline connections.

Phones themselves have evolved - many are now small, powerful computers that are constantly connected to the Internet.

Tethering

Tethering is the act of connecting your phone to your computer so the computer can use the phone's Internet connection. Sometimes inaccurately described as a "modem" in these situations, the phone simply acts as a gateway connecting your PC to the mobile data network.

Summertime is vacation time for a lot of business owners, and keeping in touch with the office can be a challenge while you're on the road. Here are

Not all phones or providers support tethering. When available, it usually uses a USB cable to connect the computer to the mobile phone.

An option that's becoming more popular recently is the ability of some phones to act as a Wifi hotspot. When enabled, the phone itself becomes a Wifi access point, and laptops and other Wifi-enabled devices can connect to the Internet just as they would via any other hotspot.

Cellular Hardware

If you don't have a phone capable of sharing its Internet connection, another option are devices dedicated to providing Internet connectivity to your computer.

Many mobile providers offer USB devices that act as dedicated interfaces to the Internet using the mobile network.

Drawbacks of mobile broadband

There are two primary drawbacks to mobile broadband: Coverage, speed and cost. While decent voice service is nearly universal in all but the most remote locations in the US, good data coverage is a gamble.

It isn't uncommon for one carrier to have "four bars" of coverage in an area, and another to have barely any, so if you travel much, particularly to more rural or remote areas, cover-

age matters. You can easily try out different carriers by purchasing "reloadable" service on that carrier - if the service doesn't work, simply cancel without penalty.

Cost is another limiting factor to mobile connectivity. Most smartphones include some kind of base connectivity charge in their monthly fee, adding \$20, \$30, or more per month to the basic cost of the phone.

Free Wifi hotspots

At the other end of the cost spectrum are the networks of free open Wifi hotspots that you can find across the country.

Be it Starbucks, McDonald's, local coffee houses, restaurants, bookstores, and more, many retail businesses provide Wifi as perk of doing business with them.

If your travels take you along routes populated with these types of establishments, you can travel from one to the other, taking advantage of their connectivity as you go. While technically free, the assumption is that you're a customer - so at least buy a cup of coffee.

The drawbacks here include security and possibly speed. Depending on how heavily used the location is, your speed of access may depend on how many other users you're sharing the connection with.

We're proud to partner with the computer industry's leading companies:

Microsoft Partner



**Microsoft®
Small Business
Specialist**

Business Partner



Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Server Maintenance: Why We Do What We Do

*by Frank Wright,
Service Manager*

Most small businesses have onsite servers, which is a change from years past when small businesses didn't see the benefit of having a server in place and instead depended on sharing within a workgroup.

With the great benefits of having a server in-place comes some additional costs to make sure your investment continues to be beneficial.

Many businesses that put a server in place are always defensive about having server maintenances done within a month after putting a server in place.

The number one phrase we hear after putting a new server in is "Are you sure that needs done, we just put that server in?"

The problem with taking this approach with your new server is that you already put a substantial investment in your new hardware and want it to run great for a long time.

Neglecting the server, even if it is for a short period of time, or even if it was "just put in," is dangerous. There are items that can go bad or cause problems if not addressed, even on a new server.

The first item and most arguably one of the most important are the server updates. Servers have to be kept up to date especially since they physically host your important data.

Allowing a server to become outdated is highly risky and potentially allows hackers access to your server via security exploits in the operating system, Internet Explorer,

Adobe, etc. If these items go without their security updates you run risk of data breach.

The second item that is one of the most important items that we check is the health of your RAID disks.



possible to have the RAID disks fail and lose all the data because it was not caught.

We have had clients bring in computers that are brand new with failed hard drives so it can and does happen at any time, even when they are brand new.

During our maintenance we also go through the logs on the system carefully combing over the entries looking for any instances that could potentially indicate a problem or an upcoming problem if let go.

If this is not done your server could be showing that it is starting to have problems but you would never know it until it is too late.

One of the logs, the Security Log, allows us the ability to see whether or not your server has had unauthorized attempts to login to it. Yes, we mean hackers trying to get in your sever and to your private data.

These are just three of the numerous areas we check with the server maintenances to ensure that your server, whether new or old, is running properly and continues to do so for years to come.

If a server is not properly maintained, it can degrade quickly into an almost useless piece of equipment and the investment you put into becomes a waste as well - not to mention the potential data loss.

Most servers (at least the ones we install) have a RAID configuration of some sort configured to help protect your server in the event of a hard disk failure.

Hard disk failure is not a matter of if it will happen but rather when it will happen.

Since this is the case we generally set our clients up on a RAID 5 configuration which allows up to two RAID disks to fail at different times.

The redundancy provided by RAID 5 configurations allows for a large amount of protection from data loss but does not guarantee it. If a business's server was not having regular maintenances done it is very

Don't waste your company's hard earned money! Invest in systems maintenances, every month. This is the only way to prevent major issues with your server and avoid data loss or compromise.

Create new service requests, check ticket status and review invoices in our client portal:

<http://www.TechSupportRequest.com>

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.



Mobile Devices: BYOD Deserves Special Consideration

by **Jeremy Miller,**
Technician

A good majority of people now bring a device of their own to work and many even use their own device at work. There are many reasons that this could be good or bad or down right terrible.

There are always inherent risks when employers allow employees to use a personal device at work especially if the device attaches to the network or has confidential data stored on the device.

Allowing employees to bring their own device can be very beneficial to your organization.

If you choose to allow devices you must understand the risk and create rules that keep the device from being used maliciously.

It is best practice to create an Acceptable Use Policy for Devices. This will cover a variety of things including:

- Proper use during and after hours.
- What types of apps are allowed to be installed?
- Which type of data will the device be allowed to use.
- How to prevent abuse.

A good AUP will allow a business to allow users to bring in their own devices and use them to increase their productivity without letting the employees abuse the privilege of being allowed to use a personal device at work.

Allowing employees to bring their own device can: increase productivity at a low-cost to the business, make employees happier, and allow users to be reached at any time.

Allowing employees to bring in their own device can be bad as

well. The first reason is employees' abuse devices all the time.

In every workplace there are employees that will use their devices in a matter that is not related to work such as checking Facebook or texting when it is not necessary.

Then there are employees that will want to use their device at work and at home, but will not want to



follow the Companies Acceptable Use Policy.

This is not only disobedience but risky, because many of the stipulations in the AUP are to protect the Company's business flow. Allowing employees to bring in a device that connects to email will sometimes require an IT person to help get the email to sync with the device.

If you do not have onsite IT this can cost you money every time there is an issue with the email not syncing. The ugly part of allowing users to bring their own device is the lack of control and security.

With the lack of standardization each device is at least a little different. On top of that each app installed is a potential risk, espe-

cially the free apps that include advertising.

Risks emerge every day, this means that in order to be sure that the device is secure you will have to continuously assess the risk for each device in use.

There is always a risk that your employees could fall victim to social engineering. This is when they either knowingly or unknowingly give away confidential information to a party that is not allowed this information.

This can be mitigated by educating users on a continuous basis, a good way to do this is a lunch and learn style of meeting. All employees with a personal device being used for work should be restricted to which applications they are allowed to download.

This is because each app has its own code and permissions that are required to run it. If the permissions for the application can compromise any data at any point it should be reviewed and then allowed or disallowed.

In conclusion many companies already allow the use of a personal device for work. Trying to implement a plan after allowing the devices is much trickier because you are further limiting a user on their own device.

A plan is absolutely necessary to protect you from legal implications, and to be up front and informative of the consequences for breaking any rules outlined in the Acceptable Use Policy for Devices.

Letting your employees know what is expected will reduce the legal and liability risk that a company may face.

Visit The Tech Experts Twitter & Facebook

facebook



Name:
Tech Experts

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





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**

1206 South Telegraph Road
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Social Media Management: Think Local

Marketers seem to be hearing three words a lot more these days: "social," "local" and "mobile."

With more and more users relying on cell phones and tablets and the geo-location technology that accompanies them, more and more businesses are realizing they need to think locally.

One good way to use social media to appeal to a local audience is to develop a blog. Blog posts are excellent places to write about things specific to your local area – events, people, places and restaurants, for example.

When writing blog posts, make sure you optimize the post by using tags

that demonstrate the local nature of your business so you will benefit from your local search strategy and will be indexed in the correct manner by search engines.

Another way to better optimize your social search is to submit your profile data to local directories such as Yellow Pages and SuperPages.

Business To Business Marketing Tips

Marketing is the life blood of any business. Staying in touch with customers, prospects, and vendors is critical to the growth of your business. Here are some tips to use the technical resources available to you to promote your business.

Business Blogging

Many B2B businesses, from the manufacturers of GPS devices for vehicle tracking to the providers of credit card processing services, are blogging today for a very good reason: blogging represents real power.

When done properly, it allows B2B businesses to generate leads, brand awareness, brand loyalty and greater interest in general. And B2B blogging is not all that difficult to get right, so long as a few simple tips are followed.

Knowing your audience is a very simple but effective tip. Make sure you have done research on your target audience, either on your own or with the assistance of an Internet marketing company, and then write appropriate content to best reach those individuals.

Another simple tip is just to have a plan. It is always important to actually plan ahead when it comes to being able to offer the best content.

Plan out ideas for blog topics for at least one month in advance, and make sure that you have a backlog of post ideas so you can fill in any gaps.

Creating Compelling Email Copy

Email marketing has evolved in a big way over the last few years, and yet the fact remains that über-designed emails with lots of "bells and whistles" are meaningless without well-written content. The good news is that

in the end, writing a great marketing email all comes down to just a few simple copywriting best practices.

Writing a genuinely compelling email subject line is one such practice. The message itself might be a work of literary genius, but no one will ever read it if the subject line does not inspire the receiver to open the message and read it in the first place. Use actionable language that makes it very clear what the reader can do with the information contained in the email message and why he or she should read it.

Wherever possible, personalized emails also work well. That means more than just including the recipient's name; it means also knowing personal information about the person to whom you are sending your messages, including what he or she is likely to be interested in.

MCHUMOR.com by T. McCracken



An Earth Mover.