November 2013

TechTidbit.com

brought to you by Tech Experts

How Important Are Websites And Search Engine Rankings For Local Businesses?

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

I recently had to find a new veterinarian for my dog Daisy. She had a fairly large sized tumor in a delicate spot, and it needed to come off. Her former doctor in Ohio sold his practice, so I was searching for a local vet who could take care of the surgery and ongoing care.

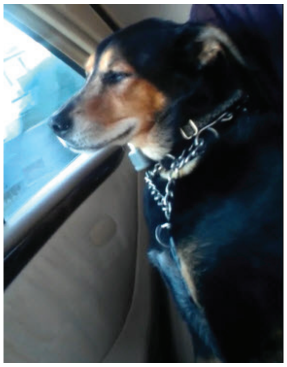
Daisy's a healthy dog, but she's getting up in years – she'll be 15 on her next birthday – so I was really concerned about the effects of anesthesia and the success of the surgery.

Of course, I spoke to friends and family for their recommendations, but I also spent a lot of time looking on my own. And where did I search? Google, of course.

We have a large number of small business clients who serve the local market area – companies like florists, tanning salons, and even a marina – and aren't interested in, or even need, the global exposure a web site gives their company.

A fresh and updated website doesn't always figure into their marketing strategy. I think that's a costly mistake. According to a report published by Google, 70% of consumers still reference the yellow pages. I was surprised by that statistic – I don't even have a phone book at home anymore.

What's interesting is that only 33% of those consumers use the yellow pages exclusively. That means that almost 70% of local shoppers are using search engines for at least part, if not all, of their buying research for local products and services.



Daisy on the drive home from surgery. She's zoned out from the anesthesia.

Google has recognized the need for local, small business search results, and has for a number of years offered Google Places and Google Local for small businesses to showcase their companies. Places or Local results point back to a company's website.

That's the important part. While I was looking for a veterinarian, I found a dozen local offices. About half of those had websites. And all but two of those websites were old and out of date. One doctor's page even had the wrong phone number on it.

Having an updated and user-friendly website is only part of doing well in local search. The other part is optimizing your site to make it index well in Google, so when consumers search for the services you provide, your site shows up at the top of the listings.

We offer both website development services, as well as search engine optimization. Pricing for a modern, user friendly website (that you can edit yourself once it's finished!) starts at just $299. If your website needs are more complex, we can handle that too – and at a very budget-friendly price point. If you have an interest in updating or modernizing your company's website, I'd welcome the chance to talk with you about it.

Daisy is doing great, by the way. Her stitches came out a few weeks ago and she's back to chasing cats in the yard and angling for cookies in the house.

Mobile Device Management Is Key In Securing Your Network

by Jeremy Miller, Technician

Mobile devices have been finding their way into the workplace since the cell phone was invented. Since the evolution of mobile devices in the workplace is rapidly growing and changing it can be hard to make sure that your device is not leaking company information intentionally or even unintentionally.

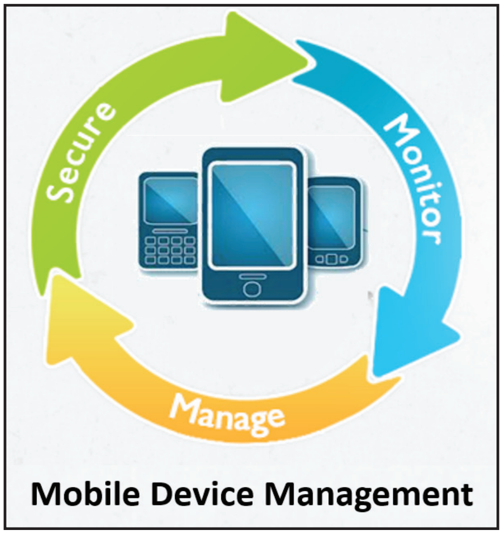
Information Technology (IT) has had to evolve alongside mobile technology and how to secure devices without restricting too much access.

There are usually two options of allowing mobile devices in the workplace. You can provide your employees with a company owned device or you can allow them to use their personal device.

Providing your employees with a company owned device allows you to monitor every detail about the phone including calls, messages, installed apps and location of the device. This is possible because the employee can expect no privacy from the company on this device.

When you allow an employee to use their own device at work you have to take their personal privacy in consideration. You might not want to monitor their phone calls, messages and apps installed.

Instead you can make the device more secure. You can install monitoring software that will allow you to lock the device if it gets lost, wipe the device if you know it may have fallen into the wrong hands, or find the device by using GPS location.



We have the ability to install our monitoring software onto any Android or iOS device and choose a profile that will suit a personally owned device, a company owned device or we can even customize a plan that will suit your needs even more specifically.

Since mobile devices are prone to getting lost or stolen they need to be protected in the best way that you can. In most cases installing monitoring software is the best solution.

This is because we can monitor the phone without interfering with the device usage. Once the device is compromised we can act quickly to get the device secured.

On the other hand if you notice an employee is acting suspiciously you can monitor their phone usage to determine if they are wasting time or acting maliciously against the company and take action before something more serious happens.

The best part about managing your mobile devices through Tech Experts, is that we are very competitive with other personal phone security managers out there in both price and features.

Our prices are very affordable and services can be easily customized to meet your needs.

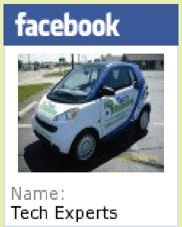
It takes just about as long as installing an app to your phone as it does to setup our management software on any mobile device running Android or iOS.

You will be able to rest assured that your mobile devices are virtually safe from data loss, your employees are using their resources and time accordingly, and in the event of an issue we will be there to assist you in any way we can.

If you are interested in trying out our mobile device management service please contact us and we will be happy to help you with any questions.

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

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 Tips For A Secure Network

by Michael Menor,
Network Technician

As the first layer of defense in your network, it is important to take a step back and review the design of your perimeter security.

To ensure a sound architecture, you want to start with what ultimately must be protected and then design your perimeter security so it can scale as your needs grow/change. Since the threats you know about and face today may not be the ones you face tomorrow, you want to be sure your design is flexible enough to meet future needs.

Think of your network perimeter like a castle during medieval times, which has multiple layers of defense – a moat, high walls, big gate, guards, etc. Even in medieval times, people understood the importance of having layers of security and the concept is no different today in information security. Here are four tips:

Build layers of security around your castle

No defense is 100% effective. That's why defense-in-depth is so important when it comes to building out your security. The traditional first line of defense against attacks is typically the firewall, which is configured to allow/deny traffic by source/destination IP, port or protocol.

It's very binary - either traffic is allowed or it's blocked by these variables. The evolution of these network security devices has brought the Next-Generation firewall, which can include application control, identity awareness and other capabilities such as IPS (Intrusion Prevention Systems), web filtering, advanced malware detection, and more baked into one appliance.

Whether or not it's part of your firewall or a separate device, IPS is another important perimeter defense mechanism. Having your IPS properly optimized and monitored is a good way to catch attackers that have slipped past the first castle defense (firewall/router).

The popularity of moving more into the cloud has brought cloud-based malware detection and DDoS (Distributed Denial of Service) services. Unlike appliance-based solutions these are cloud-based services that sit outside your architecture and analyze traffic before it hits your network.

Harden your device configurations, software updates and security policies

Here is where we start building those walls to prevent attackers from getting inside the castle. The first line of defense typically involves network security devices such as routers, firewalls, etc. which each act like the guards, gate, moats, etc. of long ago.

For each layer of security, you want to ensure they are running the most up-to-date software and operating systems, and that devices are configured properly.

A common misstep occurs when organizations assume they are secure because of their many layers of defense, but a misconfigured device is like giving an attacker a key to the castle. Another important practice is to tighten security policies (of course without impacting the business), so for example you don't have a router allowing just anyone to Telnet to it from outside your network.

Enable secure network access

While firewalls, routers and other security layers are in place to prevent unauthorized access, they also enable access that is approved. So how do we let authorized personnel into the castle? The drawbridge of course! Next-generation firewalls can help here by scanning inbound and outbound user traffic, all while looking for patterns of suspicious behavior.

Password complexity also plays a big part in Secure Network Access. Ensure your users are following these common rules.

- The password must be exactly 8 characters long.

Continued on Page 4

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

BlackBerry To Profit From Patents

by David Stone,
Technician

After a little over a decade of being a main mobile power in the business world, Blackberry (NASDAQ: BBRY) is fading to black.

The smartphone and tablet manufacturer is getting edged out by an array of factors: First they waited too long to release a device that could compete with Android and iOS, and then fell short on innovative features and operability. Secondly, they failed to market their devices to generate the kind of "tech buzz" needed to drive consumer sales these days.

While Blackberry reigned supreme as the go-to business message service and mobile emailing solution, they were surpassed by changes in industry and social popularity.

Perhaps they made changes too little too late, or perhaps they thought that their grip on the business world would ever cease. Either way, they will forever be an example of how refusing to adapt and change or not being able to see the coming change will extinct your business.

The announcement of profit losses was preceded by a work force reduction plan and the possibility of going private. Both indicate a company in turmoil, not a tech giant about to reinvent the way people connect and share data. The future for new devices looks bleak at Blackberry, but the future of the company looks like it might have some options that provide low-maintenance profitability.

In addition to being the 6th largest manufacturer of mobile devices (smartphones & tablets) Blackberry also provides mobile internet service to 91 countries on a worldwide network of over 500 mobile carriers.

Blackberry also holds a lot of proprietary patents, which much like Microsoft will generate plenty of income with little to no cost. This would essentially turn the company into a technology holding company, with a focus on maintaining licensing not developing new hardware. In effect, this would hand the company over to the lawyers and wrestle it away from the engineers. That does not bode well for any company that wants to be a industry trend-setter.

With stiff competition from Android and iOS, a former industry standard in the world of mobile computing is all but gone. Perhaps it will remain in the ring for a few more rounds with a cult-like following of users, or maybe they will break into the services sector and resurge as a mobile-enhancement services company.

Top Tips For A Secure Network, Continued From Page 3

- It must contain at least one letter, one number, and one special character.
- Two of the same characters sitting next to each other are considered to be a "set." No "sets" are allowed.
- Avoid using names, such as your name, user ID, or the name of your company or employer.
- A new password shouldn't be too similar to the previous password.

Another way to have secure access from the outside through the perimeter is to install a VPN (Virtual Private Network) that is configured to allow encrypted communication to your network from the outside. Utilizing two-factor authentication with a VPN contributes towards ensuring the integrity of the users making the request. This is external-facing to your network and allows users to tunnel into your LAN (Local Area Network) from the outside once the appropriate measures are taken to secure access.

Create and segment the DMZ

If firewalls, routers, web filters, etc. are the guards, moat, gate, walls of a castle, then the DMZ (De-Militarized Zone) is like the courtyard once inside the castle – another area before the private quarters.

When creating a DMZ, there should be at least a front-end firewall for the external traffic and a back-end firewall for the internal traffic. Firewall rules should be optimized and tightened on all publicly available systems to allow traffic to only the necessary ports and services in the DMZ. From an internal perspective you also want to limit who can access systems within the DMZ. One approach is creating firewall rules to only allow the source IP addresses and port to the specific server and then adding proxies in the network from which admins are allowed access to the systems.

Segmenting systems within the DMZ is also something to strongly consider so that if a system is breached in the DMZ, it can't spread as easily. For example, you don't want a web server passing data to an application or database server in a "public DMZ." Configuring systems within different VLANs (with a layer 3 switch) will help you isolate and respond to incidents if a server in a DMZ is compromised.

A sound network security perimeter architecture requires multiple layers of defense, up-to-date and hardened policies and controls and segmentation. All of these things make it harder for an attacker to gain access to your crown jewels and easier for you to isolate and respond to breaches when they occur.