July 2016

TechTidbit.com

brought to you by Tech Experts

How to Build A Strong Online Presence For Your Business

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

Statistics released by Google confirm that 97% of consumers now use online search to find local businesses. So what does this mean for your company?

If you want to reach potential customers, you absolutely must have an established online presence. This has two main benefits. The first involves outbound marketing. A functional website will reinforce your brand, explain your products and services, and communicate how you can solve your customer's problems. Second, establishing a portal of high-quality online content, known as inbound marketing, will help you establish your brand as an authority and will attract new customers.

There are three simple steps involved in creating a functional and effective online presence.

Create a website

It doesn't matter how small your business is, every business needs a website. It doesn't need to be fancy or complex; you just need a basic online shop front that provides your potential and existing customers with the information they may need about your business.

Creating a website may seem daunting. However, in reality, setting up a basic site can be very easy. There are even free online tools available, such as WordPress, that you can use to create a website quickly and easily with no cash outlay.

A premium version of WordPress is also available, if you want to add additional functionality, such as online shopping.

Search engine optimization

You will need to do a bit of work to make sure your website can be found by search engines, such as Google.

This involves something that is known as search engine optimization (SEO), which involves creating a website that is search engine friendly so that it appears in the top search engine rankings.

When customers search for a keyword related to your business, your website should appear at the top of the results.

SEO is important because the higher your website ranks in the search results, the more people will visit it, and the more sales you will make.

SEO is an ongoing process. You need to continually invest in new content and monitor how your website is performing in the search engine rankings for your target keywords.

Establish a social media presence

Social media connects you with your customers and allow you to interact with them. Establishing relationships on social media channels helps to build loyalty, increase revenue, and engage with your customer base.

There are many different social media channels available, the most popular of which are Facebook and Twitter.

However, the platform that is most suitable for your business will vary according to what you do.

For example, if you sell visual products or services, such as handbags, food items, or interior design, photo-sharing networks, such as Instagram and Pinterest, will be of most use. Alternatively, if you want to top the rankings in local search, a thriving Google+ account can help.

It doesn't matter how small your business is, every business needs a website.

Go Phish: Keeping An Eye On Your Email

"A largely common way to decipher what's real and what is not is the sense of urgency that these messages will have."

Brian Bronikowski is Field Network Engineer at Tech Experts.

Email phishing scams are nothing new in the IT world. There are always new messages coming through that seem more and more realistic. When you add this to your messages from princes, lottery winners, and investment requests, your inbox can grow rapidly.

There are a few ideas that phishing scams use, but there are also ways to look out for them.

There are a few different types of phishing on the Internet. Some will focus specifically on an organization or group.

Others are more generic. Some will take an idea that could apply to those with a certain attribute of family or business life. There are even attempts that pinpoint the "higher ups" in certain organizations and businesses.

So what are ways to notice these scams? A largely common way to decipher what's real and what is not is the sense of urgency that these messages will have.

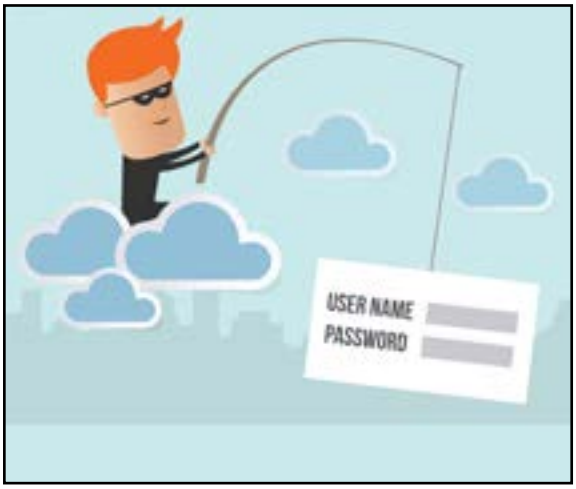
They require important personal information as quick as possible. This urgency is used to put your caution aside so you don't lose out on whatever they are threatening.

These will also be very broad so it seems you're not the only one receiving this message – and of course, you aren't.

Either way if someone states they are deleting your emails, suing for some unknown offense, or offering part in a larger grouping of people, it's likely that you need to take a minute and think about what's really going on.

Another easy method that cannot be stated enough is the amount of spelling and grammatical errors.

Professional emails are generally well-groomed and checked over by the sender. Phishing scams, however, seem to have a commonality in that they never seem to read properly. These will have easily noticeable spelling errors.



You can also notice that sentence structure is off and it is very broken in general. While people can make spelling mistakes and others may not be the best proofreaders, there is always a need to be on the lookout for errors. In the scenarios where a business or group is targeted, there may be a few other steps to take.

Emails may be sent that were not expected by the receiver. Perhaps it is an event you did not hear about beforehand. Other times, and commonly as of late, there will be a document that the receiver was allegedly "expecting."

Other times, they will use the tactics mentioned previously such as the urgency or broadness. While none of these are good to open, it is especially dangerous to open any attachments that are in the spam messages.

These can lead to ransomware and cryptoware infections that cost a lot more than the annoyance of seeing the messages.

Luckily, for all of these issues, there are ways to prevent the messages as a whole. Most large email providers will have some level of protection.

The messages will instead be directed towards your junk folder in hopes you won't accidentally click on them.

For those that use hosted services, providers are likely taking further steps to prevent these messages. Tech Experts is one of these providers; we are able to host email and protect against a large majority of these threats.

Regardless of what you use for email services, it is always important to keep in mind what's real and what's too good to be true.

Keeping that in mind can be the deciding factor between infections, data loss, or identity theft.

Is Your System's Backup Plan Working?

Luke Gruden is a Help Desk Specialist at Tech Experts.

At any moment, anything can happen that can cause your computer to fail and lose months - if not, years - of company data. This is why it's important to have some sort of system backup in place so that files can be retrieved in case anything ever does happen to your computer or network.

Without a backup, recovery often isn't possible and when it is, it's often more expensive than having a long-term backup solution in place.

Some believe that just because they have a backup solution, they've covered their bases. If a computer goes down, they're still safe.

Well, what about a fire in the company building? What if both your backup device and your computer are gone? What if the cloud server goes down and your computer goes out around the same time? Seems unlikely, but it can happen.

Natural disasters like flooding or lightning storms, accidents such as fires or the destruction of physical property, human influence like a tampering ex-employee or a ransomware infection… these things typically don't give you enough warning to move your files somewhere safe. No matter what single backup solution you might use, there is a situation where it can fail.

This is why redundancy of backups is important, such as the cloud or another device. With different backup plans utilizing different locations, you can make sure that no one natural disaster or ransomware infection can stop your business for long. If anything should happen, your data will be untouched somewhere.

It's recommended that you have at least two different backup plans in different locations. However, the more, the better. Having three different backup plans in different locations like the cloud, an offsite backup, and onsite is optimal in making sure your data is safe.

If your company data is important (which it is), there should not be a second thought in backing it up.

Remember that the more redundancy you have with your backups, the chances of losing your data drop significantly. Also, check to make sure your backup services are working and up to date as often as possible.

That way, you will not have any surprises when you least expect it and when you most need your data. At Tech Experts, we offer backup solutions that include status notifications for every backup.

It seems like we talk about this issue a lot and it's true. We bring it up so often because disasters do happen and there have been companies that have been crushed by not having a good backup plan. Don't let your workplace be one of them.

Take a moment and really consider how much effort you would have to put in to bring your business back up to speed after a data disaster. As always, work with your IT department and figure out what plan is best for your company before committing to anything. Interested in learning which backup solutions would best suit your business? Contact Tech Experts at (734) 457-5000.

"With different backup plans utilizing different locations, you can make sure that no one natural disaster or ransomware infection can stop your business for long."

What's The Best Way To Prolong Laptop Battery Life?

While experts' advice sometimes conflict, with proper care, your laptop's battery should last you a few years; without it, it may quickly begin losing charge or need to be charged more frequently.

The confusion on this arises from the different care required for older, nickel-based batteries that lasted longest when completely drained and then completely charged. While it's inevitable that you'll occasionally use up all the charge or leave your laptop battery charging beyond reaching full capacity, there is a bit of finesse involved in getting the most out of your lithium battery.

First of all, don't drain your battery level below 40 to 50% on a regular basis. A partial discharge is far less stressful on your battery, ultimately prolonging its life. This is for your regular charging activity. Once every month or so, however, you should use up every bit of battery life. Since most lithium batteries these days are "smart" ones, they are able to relay information about the remaining amount of charge. By completely draining the battery periodically, it recalibrates this system, making it more accurate in the long run.

Secondly, you should not regularly charge your laptop battery to full capacity. The longer your battery charges, the higher its temperature gets. This adversely affects your battery's capacity to hold a charge.

Once that capacity is lost, it is gone forever. So, taking this all into account, the best way to prolong laptop battery life is to maintain a charge between 40 and 90% at all times, except for a complete drain monthly.

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

How An End User Might Accidentally Undermine Your Security

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

If you're like every other small business out there, you know that the more employees you hire, the more technology that you have to procure. However, when you have more end-users, you provide more avenues for threats to slip into your network infrastructure unnoticed.

When all it takes is one simple mistake from a single end-user, how can you minimize the chances of falling victim to an untimely hacking attack? We've put together a list of honest mistakes that any end-user can make - and how they can be prevented.

Clicking on malicious links

With so much information on the Internet, it's easy for an employee to search through countless pages without any regard to the sites and links that they're clicking on.

You need to emphasize the importance of safe browsing, including double-checking the destination of a link before clicking on it. You can do so by hovering over the link and looking in the bottom-left corner of your browser.

Using weak passwords

Employees frequently use passwords that aren't strong enough to keep hackers out. Often times, they'll simply use something of personal significance, like the name of their pet or a specific date.

This isn't the right way to approach password security. Instead, users should attempt to put together passwords that are private, randomized strings of numbers, letters, and symbols.

Losing unencrypted devices

It's not unheard of for an employee to use company devices in public places. If they accidentally leave their smartphone on the bus or their tablet on a park bench, there's always the risk that it can be stolen.

Unless you practice proper encryption protocol, any information available on the device can be accessed by the person who finds it, be it a good Samaritan or a tech-savvy thief.

Implementing unapproved solutions

Some employees simply prefer to use solutions that aren't provided by the company to get their work done. The problem here is that the employee is moving forward without consulting IT about it and that your data is being used in a solution that you can't control.

Plus, if the employee is using free or open-source software, these often come bundled with unwanted malware that can put your data in even greater peril.

Personal email use

It's one thing to check your personal email account while at work, but another entirely to use your personal email account to perform work purposes.

As the recent debacle with Hillary Clinton shows, people don't take kindly to sensitive information being leaked via an unsecured email server that their organization has no control over.

Add in the fact that personal email accounts are often not as secure as those in a professional productivity suite and you have a recipe for disaster. You need to reinforce that your team should keep their work and personal email separate.

Leaving workstations unattended

Besides the fact that some tech-savvy employees are practical jokers, it's a security risk to leave a workstation unlocked and unattended for long periods of time.

Imagine if someone from outside of your organization walked into your office and accessed confidential files without authorization; that's on the employee who got up and left the device unattended.

Encourage your employees to always log off of their workstations, or at least lock them, before stepping away from it. User error is a primary cause for concern among businesses, but it can be mostly avoided by providing your staff with the proper training. For more information on IT best practices, give us a call at (734) 457-5000.

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