May 2015

TechTidbit.com

brought to you by Tech Experts

How Can You Use Google Trends For Small Business?

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

Google Trends is a tool that has been around for a while, and has great potential for improving exposure and sales for businesses. It is entirely free to use, and its simplicity makes it accessible to virtually anyone with basic computer knowledge.

Here are some specific ways in which you can use Google Trends to enhance your small business practices:

Brainstorming Topics

For instance, if your business website contains a blog, it's common to quickly run out of content ideas that will not only interest your readers but also tie into the products or services your business offers.

Choose a phrase that describes a broad idea for a blog post, and Google Trends will show you how popular that phrase is and also suggest related topics. With one simple search, you could potentially come up with ideas for dozens of different blog posts, and relevant content is the best way to build your business website.

Keyword Research

Although you may want to continue using other keyword research tools to develop your SEO practices, Google Trends can give you a general idea about what keywords people are currently searching for on the web.

As when you use this tool for brainstorming, you can get ideas for other keywords that perform as well or possibly better than the original word or phrase you searched for.

Industry/Brand Research

You can't stay on top of the competition unless you know what the competition is up to and how consumers respond. Search Google Trends for your industry field, and see what brands show up the most to gauge your performance against others. Also, you can compare various brands within your industry to see what their related concepts suggest about their current practices.

What's Trending

With the name Google Trends, you'd certainly hope this tool would show trending searches and topics, and it doesn't disappoint on that front.

If something has gone viral (or at least enjoyed higher than average popularity) within your business industry, this tool can give you a heads up so you can use it to your advantage.

Sentiment Analysis

Not all exposure is positive exposure, so you don't necessarily want to hop on a particular keyword bandwagon just because it's popular.

The Google Trends graphs show the number of searches for a specific keyword, and correlate to news stories associated with the searched word or phrase. That way, you can avoid implementing keywords that have negative connotations.

Data Breaches And The Building Blocks Of Cyber Security

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

The data breaches at Target, Home Depot, Staples, Michaels, Anthem, and Sony Pictures Entertainment are just the tip of the iceberg and the stakes are very high. They're costly for both businesses and customers and once the breach is announced, customers often terminate their relationship with that business.

You may ask, "What constitutes a data breach?" It is an event in which an individual's information, including name, Social Security number, medical record and/or financial record or debit card is potentially put at risk. This can be in either electronic or paper format. The data set forth in this article is based on Ponemon Institute's "2014 Cost of Data Breach Study." Ponemon conducts independent research on privacy, data protection and information security policy.

New methodologies developed by the National Institute of Standards and Technology (NIST) and other industry standards bodies, such as the Department of Health and Human Services (HHS), are being implemented by many organizations, but best practices for addressing cyber security threats remain vague.

So what can be done to minimize cyber security threats? An effective starting point is to focus on the following essential building blocks of any cyber threat defense strategy.

Most organizations rely on tools like vulnerability management and fraud and data loss prevention to gather security data. This creates an endless and complex high-volume stream of data feeds that must be analyzed and prioritized. Unfortunately, relying on manual processes to comb through these logs is one of the main reasons that critical issues are not being addressed in a timely fashion.

Implementing continuous monitoring, as recommended by NIST Special Publication 800-137, only adds to the security problem as a higher frequency of scans and reporting exponentially increases the data volume. Data risk management software can assist organizations in combining the different data sources, leading to reduced costs by merging solutions, streamlining processes, and creating situational awareness to expose exploits and threats in a timely manner.

One of the most efficient ways to identify impending threats to an organization is to create a visual representation of its IT architecture and associated risks.

This approach provides security operations teams with interactive views of the relationships between systems and their components, systems and other systems, and components and other components. It enables security practitioners to rapidly distinguish the criticality of risks to the affected systems and components. This allows organizations to focus mitigation actions on the most sensitive, at-risk business components.

Effective prioritization of vulnerabilities and incidents is essential to staying ahead of attackers. Information security decision-making should be based on prioritized information derived from the security monitoring logs. To achieve this, security data needs to be correlated with its risk to the organization. Without a risk-based approach to security, organizations can waste valuable IT resources mitigating vulnerabilities that, in reality, pose little or no threat to the business.

Lastly, closed-loop, risk-based remediation uses a continuous review of assets, people, processes, potential risks, and possible threats. Organizations can dramatically increase operational efficiency. This enables security efforts to be measured and made tangible (e.g., time to resolution, investment into security operations personnel, purchases of additional security tools).

By focusing on these four cyber security building blocks, organizations can not only fulfill their requirements for measureable risk reporting that spans all business operations, but also serve their business units' need to neutralize the impact of cyber-attacks.

These methodologies can also help improve time-to-remediation and increase visibility of risks.

The Reality Of Microsoft EOL Software

Scott Blake is a Senior Network Engineer with Tech Experts.

As in life, all good things come to an end. This fact is also true in the software world. When a software company decides to move on from outdated versions of its software they schedule an EOL or End of Life date.

This is set to allow businesses and home users time to plan and ready themselves to upgrade to the most recent versions.

With 90% of the world's computers running some form of Microsoft software, no other company in the world has more of an impact when setting EOL dates than Microsoft.

From Office software suites to operating systems for desktops and servers (and even cross platforms such as Office for Apple-based computers), Microsoft software is everywhere.

This alone is the number one reason for preparing and upgrading before an EOL date is upon you. There is no greater example of this as when the EOL date for Windows XP arrived.

Companies that made the migration to Windows 7 well in advance were able to test their company software and hardware, as well as communicate with their vendors to secure working upgrades to both. Those that didn't suffered productivity and business loss due to unneeded and unplanned downtime to make the necessary upgrades and changes.

But for the basic home user, this was a time of doubt. Many users didn't want to (or have the means to) replace all of the outdated hardware or software.

Spending several hundred dollars on new software and hardware just to be able to receive security updates and patches seemed a little excessive to most home users.

However, keeping security and your data safe is another reason to make sure you make migration plans.

In most cases when an EOL date has come and gone, so has any and all support for your software and hardware. Other software and hardware vendors will soon follow suit and discontinue support for their products that are installed on systems running non-supported software, including operating systems.

Anti-virus software companies are usually the first to discontinue their support. After all, if the operating system is no longer receiving updated security patches, it becomes difficult to continue to support their software.

Computer systems running EOL software will become major targets for hackers and malicious malware. Your personal data will be at risk.

The truth is it's not the intent of companies like Microsoft to be malicious when ending support for their products.

No matter how popular they may be throughout the world, it's a business decision. For any company to grow, they must keep developing and growing their products.

This development and growth is expensive and requires a large percentage of their resources. Continuing to support outdated software and hardware would limit these resources.

This would cause development overhead to rise and, in turn, make that $39 inkjet printer cost $89 or raise the price of that $119 operating system to $199.

By ending support and moving forward, companies such as Microsoft are able to develop new and exciting hardware and software for both the largest of companies and the smallest home user while keeping prices affordable to all.

Some important future EOL dates to keep in mind:

July 15, 2015

The end for support for Microsoft Server 2003 and 2003 R2

April 10, 2017

The end of support for Windows Vista (all versions)

October 10, 2017

The end of support for Microsoft Office 2007 (all versions)

January 14, 2020

The end of support for Server 2008

October 13, 2020

The end of support for Microsoft Office 2010 (all versions)

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

Security Tips To Keep Your Mobile Phone Secure

We've all seen the stories about celebrities getting their mobile phones hacked and having their private photos splattered all over the web.

Although you may think there is nothing of real interest on your phone, you are still at risk of security invasion. Any number of people could have motive to do so from exes to a colleague who perceives you as a threat, and even innocuous content on your phone can be taken out of context to reflect negatively on you in general.

Use some of these simple tips to protect your mobile phone and reputation:

Passwords

Your passwords are your primary defense against would-be hackers – from your lock code to email account password. Don't share your passwords with others. Also, make sure your passwords aren't easily guessed, such as your pet's name or child's birthday.

A secure password may not be as easily remembered, but it is far harder to hack. Finally, shield your phone's screen when entering passwords in public lest onlookers take note of which buttons you push.

Clear Out the Cobwebs

In addition to creating more storage space on your mobile phone, it is just wise to remove old text conversations, photos, and other data periodically.

Back up the things you want to keep onto other devices, so you can access them later. With all of the excess stuff you don't use on a regular basis gone, you leave less for hackers to work with if the security of your mobile phone is breached. In the event of being hacked, you would also likely lose all of those things, so backing such info up protects you twofold.

Beef Up Security

Take advantage of the lesser-known security features of your mobile phone. For example, turn off the Discoverable mode on your Bluetooth.

Look on your phone under Security to see if there are already included options, such as an automatic lock screen that activates after a certain period of inactivity.

There are also applications you can download to increase the level of security on your phone, including apps that allow you to access and control your phone remotely in the case of loss or theft.

Major Microsoft Windows Vulnerability Discovered

Microsoft recently released details about the newest vulnerability (MS15-034) in the Windows HTTP stack's armor. With other recent problems in Microsoft patches, the problem may have been downplayed a bit to save face. This vulnerability, however, is more serious than it initially seemed.

The MS15-034 vulnerability is widespread. Although Windows servers are most at risk, this problem affects most products that run Windows. The chink in question lies in the HTTP.sys component, which is a kernel-mode device driver that processes HTTP requests quickly.

This component has been an integral part of Windows since 2003 and is present in all versions up to Windows 8.1. This means that any device running Windows without up-to-date patches is at risk.

It isn't difficult to exploit this vulnerability. The only thing Microsoft is divulging about how MS15-034 can be used to compromise devices is that it requires "a specially crafted HTTP request." It seems that this information is deliberately vague.

All one has to do is send an HTTP request with a modified range header, and access to data is granted, although sometimes limited. A similar attack was documented in 2011 on the Apache HTTPD Web server that was later patched,

There is good news though. As in other areas of life, prevention is far more effective than trying to deal with a problem's aftermath. It isn't difficult to protect your devices from the MS15-034 vulnerability.

The first step is to ensure that your server has the latest updates that include the patch to fix the problem.

If your server hosts a publicly accessible application, you can verify your server's vulnerability by going to https://lab.xpaw.me/MS15-034, enter your server's URL, and press the Check button for an instant report on your site.

If you then see the report that the website has been patched, you're safe; otherwise, that particular system will need to be patched.