Is Your Company Getting Slandered Online?

New "Online Identity Managers" Are Becoming A Must For Business Owners Who Need To Keep Their Online Reputation Clean...

A recent front-page story in the Washington Post brought to light a fast-growing trend in today's digital world: online identity management.

According to the article, Sue Scheff, a consultant to parents of troubled teens, was getting slandered online after one of her clients turned on her, calling her "a con and a fraud," and accusing her of taking kickbacks and destroying people's lives. Negative comments were being posted on online bulletin boards, forums, and threatening videos were posted up on YouTube for the world to see.

Even though Scheff sued for defamation and won an $11.3 million verdict, the attacks worsened. To resolve this situation, Scheff was forced to hire ReputationDefender, a PR firm that cleaned up her reputation online.

While the costs for hiring this firm were steep (reputation management firms charge $15,000 to $100,000 for their services), the cost of her time, litigation and reputation make their fees seem like a drop in the bucket.

So what should you do if you are an average Joe small business with limited resources? Fortunately, an ounce of prevention is worth a pound of cure, and you can easily monitor your image online for free with a few simple steps.

First, the easiest way to check your online reputation is to Google your name or the name of your company and see what appears. Next, set up a Google Alert on your name and your company name. You'll be alerted by e-mail whenever you or your organization has been mentioned in a blog, by the media, or in an online forum.

Next, make sure your web site and your company is coming up first in search engines. If you own the top positions online, negative media may not show up on the first listing when your name is Googled.

To do this, create a profile of your expertise using social bookmarking tools and news aggregators such as del.icio.us and Newsvine.

Contribute to online forums and write articles for user-generated content sites such as Squidoo. You can even create book and product reviews at Amazon.com to help es-tablish your authority on a particular topic or subject matter.

You should also create a blog for yourself and your company, and then link that to your main web site. Tech Experts can help you set up a blog using your existing domain name. Post to your blog frequently and make sure your posts are key-word relevant.

Other obvious ways to put a positive spin online about your company is to create content pages on social media sites such as YouTube, Facebook and MySpace.

Finally, be very careful about post-ing any incriminating evidence about you or your company or sending e-mails with incriminating informa-tion, tasteless jokes, or messages that could easily be misconstrued.

You don't want a search on your name to bring up pictures of you in compromising situations or sexist, racist, or off-color jokes you thought were only being sent to your friends. If you wouldn't want it posted to a billboard, don't post it or send it via e-mail.

Google Alerts currently offers 6 variations of alerts - 'News', 'Web', 'Blogs', 'Comprehensive', 'Video' and 'Groups'.

- A 'News' alert is an email aggregate of the latest news articles that contain the search terms of your choice and appear in the top ten results of your Google News search.
- A 'Web' alert is an email aggre-gate of the latest web pages that contain the search terms of your choice and appear in the top twenty results of your Google Web search.
- A 'Blogs' alert is an email ag-gregate of the latest blog posts that contain the search terms of your choice and appear in the top ten results of your Google Blog search.
- A 'Comprehensive' alert is an aggregate of the latest results from multiple sources (News, Web and Blogs) into a single email to provide maximum coverage on the topic of your choice.
- A 'Video' alert is an email ag-gregate of the latest videos that contain the search terms of your choice and appear in the top ten results of your Google Video search.
- A 'Groups' alert is an email aggregate of new posts that contain the search terms of your choice and appear in the top fifty results of your Google Groups search.

Rebate Alert! Don't Get Ripped Off!

The offers are irresistible but misleading; retailers advertise after-rebate prices on hardware and software to grab your attention and get you to buy. But are you really getting the bargain you expected?

They're Counting On You To Forget

According to the NPD Group, a global market research firm, almost one-third of all computer products and twenty percent of all consumer electronics are sold with a rebate. Manufacturers use rebates as an easy way to offer discounts without actually having to take the full financial hit; that's because thirty to fifty percent of the buyers never attempt to redeem them and therefore end up paying full price for the merchandise.

Get Ready To Jump Through Multiple Hoops

To further tip the scales in their favor of not having to pay out, some manufacturers and retailers are imposing impossible restrictions, complicating the process to request a rebate, delaying payments, and creating other barriers that make it difficult to get your money. All of these are delay tactics to get you to give up on the idea of getting your rebate out of frustration.

New Laws Protect You

With consumer complaints to the FTC and Better Business Bureau piling up, regulators have tightened the rules around advertising rebates.

Last year, the Federal Trade Commission settled its first dispute with a Dallas-based CompUSA store for knowingly advertising rebates from computer peripherals manufacturer Qps Inc., even though they knew this manufacturer wasn't fulfilling on the rebates advertised.

After this settlement, CompUSA was not only required to advertise the time frame for securing the rebates advertised, but also had to take financial responsibility for any rebates not paid during the promised time frame.

Even though the government is on your side, getting stuck in the middle of a rebate war is very frustrating and a huge waste of time. If you are going to try to cash in on a rebate, here are some tips that will help.

5 Tips To Collecting Your Promised Rebate

1. Follow the rebate instructions carefully. Many manufacturers will reject a rebate over a tiny technicality. That means reading the small print and following the instructions to the letter.

2. Make a copy of all the paperwork, receipts, and documents before mailing them off. Some manufacturers may request the original receipt; if you mail in your only copy, you could be out of luck if it gets "lost" in the mail. Which brings us to tip #3...

3. Mail your rebate via certified mail to have proof of delivery. Schedule a reminder to yourself to call the company if your rebate doesn't show up within the time frame promised. Most companies will have a web site or toll-free number to call to track your rebate.

5. If the manufacturer rejects your rebate or is holding your check, let them know you plan on contacting the FTC or the BBB. Ask the people you speak to for their names and ask to speak to their supervisor.

Are Your Co-Workers Stressing You Out?

It seems like every office has at least one jerk, loudmouth, or snooping pest that drives everyone crazy. Even if they are only mildly annoying, interacting with them on a daily basis can be incredibly stressful.

What are some of the things that co-workers rate as the most annoying? Loud cell-phone talkers, habitual space-invaders, and general rudeness and inconsiderate behavior towards others.

According to one ABCNEWS.com story titled, "Trapped in co-worker hell," co-workers' annoying habits are the #1 source of workplace stress (survey by www.truejobs.com).

Nearly 60% of the 2,200 who responded said bad habits and manners of co-workers as the cause of stress that negatively impacts their work life, and 40% said that annoying co-workers have led them to seek new jobs.

Do You Roll Out The Red Carpet For Identity Thieves?

Just about every web site you visit these days wants you to register and choose a password, especially when making a purchase.

However, if you do this carelessly, you may be setting yourself up as an easy prey for online criminals.

Although we know we should choose unique and hard to decipher passwords that contain both numbers and letters, most people still use easy to remember passwords and words for their convenience.
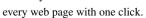
Below are the top 10 passwords used online according to PC Magazine. If you are using any of the following, you're putting a big red bullseye on your account for identity theft:

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. link182
10. [your first name]

If you want to avoid having to remember dozens of hard-to-remember passwords, Robo Form is a great FREE software you can download without having to fear adware or spyware. RoboForm was named PC Magazine Editor's Choice, and CNET Download. com's Software of the Year.

After you download the software, it memorizes your passwords and logs you in automatically to every web page with one click.

Best of all, it encrypts your passwords and generates random passwords that hackers cannot guess. You can even back up your passwords so you can copy them to another computer.

To get a copy, visit the "Free Stuff" section of our web site: www.MyTechExperts.com/freestuff

How Long Are You Going To Put Up With That Slow Computer That Is Always Crashing, Acting Crazy, and Giving You Problems?

Tiny, consistent computer problems are usually a warning sign of a much deeper problem.

That's why we encourage all of our clients enroll in our monthly system check program. Viruses, hackers, spyware, hardware failures, and software corruption are a constant threat to your network and the precious data it holds.

Ignore basic maintenance and your system will frequently crash, run slow, and put you at risk of losing data and expensive downtime.

Why should you care about this? Because there are a number of ways hackers and viruses can access your network - undetected - to embezzle your private information, steal your identity, and use your network as a conduit for spreading spam, viruses, and even illegal software.

Tape backups have a failure rate of 100% - that means all tape drives will fail at some point without warning. You don't want to find out that your backup was not working the day after your hard drive was erased.

Hardware failure and software "glitches" can corrupt your data making it useless. When this happens, you can end up spending thousands of dollars in emergency recovery services. Plus, all the tiny technical problems can end up pulling you away from your work for hours.

To make sure these disasters don't happen, there are over 67 system checks that should be done on a regular basis to secure your network and keep it up and running. Since most business owners don't have the time or expertise to perform this regular maintenance, we offer our monthly system service. Not only will your network be more secure, but we'll save you the time and aggravation of dealing with computer problems.

To find out how our system check service can help your company, call us at 734-457-5000, or e-mail us: info@mytechexperts.com.

**Want More Useful Tips?
Visit our new
Tech Experts Blog at
www.expertsguys.com**

How To Keep Your Laptop Safe and Secure

You can't beat the convenience of checking e-mail and hopping on the Internet at (Wi-Fi) hotspots found in airports, coffee shops, and bookstores. For the uninitiated, hotspots are areas where you can use your wireless laptop to surf the Web.

But the question you have to ask yourself is, just how safe are hotspots? With the proliferation of hackers, viruses and identity theft at an all time high, you're smart to be concerned. Wi-Fi spots are very attractive to hackers because they can use what's called an "evil twin" connection to access your laptop.

An evil twin is a hotspot set up by a hacker to lure people from a nearby, legitimate hotspot. For example, when you log in at your favorite coffee shop, you might actually be logging onto the evil twin Internet connection set up by the innocent-looking person working on a laptop at the next table. The most dangerous evil twins remain invisible

and allow you to do business as usual. But in the background, they record everything you are typing. Buy something online and they are recording your credit card information. Log on to your bank account, and they can grab your password.

So what can you do to make sure you are not giving an evil twin access to your laptop?

First, know the name of the hotspot you're going to use by asking someone who works there. Some businesses will give you printed instructions that include the hotspot name. But be careful. Hackers will name their evil twin network by a very similar name as the real hotspot, and may even show up as a stronger signal.

The best protection you can have is connecting via your company's VPN (virtual private network). A VPN

will protect your online information by encrypting your data and activity even if you're connected through an evil twin.

If you don't have a company VPN, you should assume that someone is looking over your shoulder and recording everything you type in. Therefore, the BEST protection without a VPN is to never type in information such as credit cards, passwords, or social security numbers when connected to a public Wi-Fi hotspot.

"He's busy right now, but I may be able to get you in to see his screen saver."