



* WHITE PAPER

Grow Your Business by Building Consumer Trust



+ Introduction

Building a successful small business web site is a huge challenge. Whether the site is merely promotional or a full-service e-commerce enterprise, you—the SMB owner—have to create an attractive and functional place with compelling content that is frequently updated. If you are new to online retailing or have only recently launched your company's online presence, some of the questions you may have asked yourself probably include:

- How can I improve incoming traffic from search engines?
- I don't have a big name brand, how can I get people to trust my web site and do business with me?
- Should I really worry about my web site getting attacked by malware?

This paper will not only answer the questions above (and many like it), it will help you learn to establish a strong online relationship with your customer that is built on trust. After all, trust is what nurtures customer loyalty.

Even great search engine optimization (SEO) can't help if users don't perceive your site as credible. They will not share valuable personal information or make a purchase if they aren't absolutely convinced of your site's authenticity. Even the most enthusiastic users can be driven away by a single virus or Trojan attack, should your site ever be compromised by hackers attacking your readers.

Now more than ever, small businesses need to implement strategies that build and improve consumer trust. Users want to be sure they haven't landed on an impersonator's counterfeit site right away. If they don't feel safe, they'll leave, and the chances are high they'll never come back...even if nothing has necessarily gone wrong.

+ This where the VeriSign Trust Seal comes in

VeriSign's Trust Seal, which is displayed more than 175 million times per day and is recognized by nearly 86 percent of consumers, can help build this sense of trust by bolstering security and authenticating your site.



+ Consumer trust is more important than ever

You don't have to be the savviest tech person around to know that online security threats are a very real thing. Just think of the various security breaches you've read or heard about in the news. Meanwhile, there is no shortage of advertisements suggesting the best products and services that can protect consumers from online fraud and other scams.

The fact is consumers and business owners understand that threats to online security are a very real thing requiring action.

- As many as 40,000 web sites are compromised per week (Google, 2009)
- \$800 billion in consumer e-commerce could be at stake if not protected (IDC, Sept. 2009)
- One in 10 US adults online have been victims of identity theft or have suffered financial losses due to their personal data being comprised, either on the Internet or offline, during a 12-month period (Forrester, Aug. 2009)

The good news is the security strategies businesses and consumer have implemented are working. Moreover, consumers are getting better at spotting the telltale signs of a compromised site and keeping as far away as possible.

- In 2008, nine out of 10 online users in the US reported that they had not been victims of fraud or identity (Forrester, 2009)

Better-educated consumers are helping to reduce online security attacks, but the services available for spotting fraud and taking action immediately to stop it are also major contributors to online safety as well.

One company taking advantage of those services is Merchant Circle, the largest social network in the United States for connecting small businesses and consumers. A small business itself, its members are provided with a web page listing and blogging, email, and newsletter applications, among other features. It estimates its membership at 1.3 million.

Though the company has had success in increasing its membership numbers, since its founding in 2005, and official launch in 2006, trust among its membership is still critical to the continued success of Merchant Circle and its 1.3 million members.

Each one of Merchant Circle's members will be able to display the VeriSign Trust Seal on their Merchant Circle profile, as part of their membership, as each individual member's site is verified by VeriSign.

Merchant Circle believes this new collaboration with VeriSign will generate the same level of trust for these small businesses' online presence that has been garnered in their neighborhoods and among their "in-person" customer base.

Meanwhile, a recent *Consumer Reports* survey found that 71 percent of online shoppers look for a trust seal before doing business with an e-commerce retailer.

+ The damaging effects of malware

Say what you will about hackers, they are a smart and diligent group of people, constantly creating new strategies for scamming or corrupting your computers, networks, and web sites with various types of malware. What is malware? Simply put, it is malicious software that comes in a variety of forms.

Having malware on your site (even if it doesn't attack the customers) will turn away those savvy enough to run security software that detects it; they might not return after such an experience. You could only lose a single sale or ad impression, or they could spread the word and you'll stand to lose a lot more.

If the malware ends up attacking users, the situation could become much worse. Depending on how much data, money, or privacy customers lose, they may never come back. Worse than the loss of individual customers is the loss of your reputation. If you experience just one malware infestation, you could become blacklisted by security software companies and even blocked by search engines. You may even be open to legal action, depending on the nature of the attack and the compliance regulations that apply to your business. At the very least, you can be sure that disaffected users will tell others to avoid your site. Many businesses never truly recover from this sort of reputation-destroying event.

+ Types of malware

Phishing

Just as the name implies, phishing is when folks with ill intentions “fish” around for your confidential information. Usually what happens is you’ll receive an email from what appears to be a legitimate company that attempts to trick you into handing out personal information, such as a credit card number or a social security number.

Identity theft

It is often your worst possible nightmare. Unbeknown to you, someone has managed to steal your personal information, such as a credit card number or social security number, and then uses this information to obtain credit, merchandise, and other services, all on your dime. Oftentimes, people don’t realize their identity has been stolen until the damage is already done.

Viruses

A computer virus is a self-replicating computer program that is bound and determined to infect as many computers as possible, destroying every piece of data it can in its wake. Many viruses are found in executable files. This is exactly why your computer prompts you with a message notifying you that you are downloading an executable file and that you are absolutely sure you trust and know the sender.

Pharming

Some describe pharming as phishing without a lure. How’s that? Well, when a scammer “phishes” for your personal information, they are usually luring you or someone else with an email that appears to have been sent from a legitimate web site. It’s an individual attack. With pharming, a large number of users can be attacked. Multiple users are essentially directed to a fraudulent website (even when they think it’s a legitimate site).

Scams

Everyone has probably received by now at least one email, typically written in all caps and in broken English, from a wealthy foreigner requesting you help him move large sums of money through your bank account and offering a significant reward in the process. Guess what? There is neither a wealthy foreigner nor reward at the other end of that email wielding a large check with your name on it.

Spyware

As the name suggests, spyware is software that spies on you. It begins accumulating bits and pieces of your online habits without you knowing it. Spyware is typically associated with adware (display advertisements) that can sometimes be bundled into other software you wish to install on your computer and starts collecting your personal information without your consent. Some can even change the configuration of your computer.

Trojan horses

You've probably heard these terms a million times, but still aren't exactly what it is. It's pretty simple. It's an email virus hidden with an email attachment. If it's opened, then it will search your hard drive for any personal and financial information it can find, such as social security numbers, PIN numbers, and checking or savings account information.

+ The impact on business

When consumers are bombarded with messages that their online security is constantly threatened, they can be hesitant to trust any kind of online transaction. In fact, 80 percent of online shoppers want more assurances that their information is secure, according to a survey published by Javelin Strategy in March 2009. Meanwhile, the web site Antiphishing.org, estimates that 48 percent of 22 million computers are infected with malware.

Convincing users to click on your listing can be tough. Building something as ephemeral and ineffable as trust is difficult, particularly if you set out to do it yourself. So when a consumer does take the leap, they need obvious indicators that a business has taken the steps needed to assure their site is a safe, trustworthy, secure place to visit and buy online. Otherwise, they aren't going to make an online purchase unless they are absolutely sure personal information, such as their account information or email addresses are safe.

This is one of the reasons why online companies BeautiCreams, Chef's Resource, and Momma's Candy signed on to have their sites authenticated by VeriSign in time for the heavy surge Mother's Day shoppers in 2010.

Their testimonials included:

- “We are confident in the VeriSign Trust Seal and building trust with our customers is a top priority of ours,” said Kandice Sullivan, owner of Momma’s Candy Store. “We want customers to know that they can do business with us and have confidence in us. We proudly post the VeriSign Trust Seal on our web site.”
- “To better serve and protect our customers we rely on the VeriSign Trust Seal to monitor our site daily for malware,” said Nancy Raby, chief executive officer of BeautiCreams.com. “The VeriSign Trust Seal helps assure our visitors that we are a company to be trusted.”
- “Chef’s Resource takes security and trust very seriously,” said Rick Smith, president of Chef’s Resource. “This is why we deployed the VeriSign Trust Seal on our web site as part of our commitment to our customers.”

*Quotes published in a MarketWatch article dated May 5, 2010

+ The impact on SEO

Having your site hacked doesn’t just threaten customer loyalty, it could destroy your company’s hard-earned search engine optimization. That is, popular search engines such as Google are now scanning for malware and blacklisting any web sites that show signs of malware. That means Google could potentially shut off your SEO traffic. Can you imagine what would happen to your company if all of your Google traffic went away?

+ We all know that SEO is the lifeblood of a company

Case Study: The Power of SEO

Company: Beaches and Bays Accommodations

Size: 15 full-time employees

Solution: To increase the business value of the corporate web site using sound design principles and search engine optimization techniques.

Results: Comparing January 2010 to February 2010

- Overall traffic has increased 35 percent
- Front page abandonment rate reduced from 78 to 32 percent

- Regular search engine traffic, as a percentage of overall traffic, improved from 5 to 25 percent
- Online request for proposals increased 600 percent
- Qualified traffic, that stayed on the site at least 10 seconds, increased from 28 to 45 percent
- Pay per click spending reduced by approximately 50 percent

The company first launched its web presence around 1994. Its goal was to increase visibility. The web site, developed by an outside contractor, continued to grow in terms of content and value. A pay-per-click campaign brought more visitors to the site, so management began to think that devoting resources towards SEO could help grow traffic further. The decision was made to redesign the site from the ground up to be more search-engine friendly and to begin a campaign of building a link network to enhance its rankings. Results have been very good: increased page views and a dramatic increase in online bookings.

+ Building trust online

Consumers and business owners might not always fully understand or have the time and resources to diligently monitor the barrage of online attacks that threaten their online security, but they have learned to recognize the signs that let them know when a site is secure. They are now familiar with the web site seals a company can earn from third-party audits of site safety.

Meanwhile, the VeriSign seal is the most recognized mark of trust on the internet.

- More than 90,000 web sites around the world display the VeriSign seal
- The VeriSign seal is viewed more than 175 million times a day
- 86 percent of consumers are familiar with the VeriSign seal

Displaying a trust seal significantly and positively influences consumers' willingness to buy the product or service offered on a web site. Case studies show a 10-34% increase in online sales and transactions when a VeriSign seal is displayed. In a recent study, 11% of respondents decided not to conduct business with the site because they did not see the VeriSign logo (US Brand Tracker Survey 2009). That same study also determined that shows that consumers who are more aware of the trust-promoting seals are more willing to shop online when a significant trust seal is present on the online store.

+ The customer life cycle

When it comes to running an online business, there is an ideal customer life cycle that all e-tailers want to achieve.

Customers find the link to your site. They see an immediate indicator that your site has been verified to be legitimate by a well-known and respected third-party site authentication service. They trust you.

Next customers will visit your web site and see the necessary indicators that your business has taken the appropriate steps required from a third-party site authentication service that once again verifies the site has been scanned for malware. Again, trust is established. You are now a trusted site they can repeatedly visit.

Everything is of course leading up to a transaction, a trusted transaction, that goes smoothly and results in repeat sales and customer loyalty.

+ Trust needs to be established fast

An important piece to building customer loyalty and increasing site visits is to establish trust even before the customer has reached your site. Potential customers are far more likely to click on links if they know a site is sophisticated enough to take security seriously and is not a phishing site, an imposter's counterfeit site, a virus delivery site, or a compromised legitimate site. Plus, if you can establish trust ahead of time, you will drive more traffic to your web site.

What's great about the VeriSign Trust Seal is it shows up as part of your listing on a search engine results page. The seal can make a real difference in producing more clicks to your website. Potential customers immediately know which web sites have been authenticated by VeriSign.

The Seal-in-Search feature is enabled by browser plug-ins that detect VeriSign trusted links in popular search engines, and also by partnerships with comparison shopping, listings, and other web sites. You can enjoy the advantage of a more trusted link that reaches customers earlier in the purchase cycle

+ Trust at the site level

Once customers have reached your site, trust should once again be immediately established.

You can do this by displaying credible trust signals that are:

- Clear
- Immediately noticed
- A well-known, reliable name or recognizable brand
- Hard-earned

+ Without trust, you're losing money

There are web sites that are so well-known (e.g. Amazon, PayPal, eBay, Macy's) that the majority of consumers don't even look for trust indicators. That's because they immediately trust that these online stores are maintaining secure sites. Why? Because they are household names they've trusted for years, and in some cases, for generations.

If you are a small online retailer, blogger, content publisher, or consultant that kind of universal presence and subsequent trust isn't so automatic. And guess what, this is costing you greatly.

Online listings compared between well-known online retailers such as Amazon and a small local business shows the small local business has to offer a significantly larger discount (on average, between 10 and 20 percent) to nab a customer's attention. That's money lost. Meanwhile, Amazon, an established, trusted site doesn't have to cost-cut to get business. People are going to continually click on Amazon because they trust it.

+ If you have to give up 10 points of margin on every sale, you could sink your business.

Small businesses get squeezed in other ways too. Suppliers often cut better deals to the well-known online retailers such as Amazon, while small or unknown businesses get nothing. You're paying more and having to give a bigger discount. Convincing customers that they are safe to do a large portion of their transactions online means a more efficient and cost-effective way for you to continue to do your business. You have to give them the evidence upfront that your on-

line business is as reliable and safe as the larger, better-known e-tailers.

+ If my site's security is threatened, what does VeriSign do?

Every day VeriSign scans your site for malware. What is malware? It's short for malicious software and includes all those threats we've already gone over (phishing, pharming, spyware, etc.) If any is found, VeriSign takes action immediately by:

- Sending you an automatic e-mail notification that malware has been detected on your site.
- VeriSign next removes the trust seal.
- The customer is then sent to the VeriSign Trust Center, which will identify the infected files, tell you the location of the malware and give you an actual view of the offending code.
- VeriSign will also provide tips for removing the malware. If necessary, you can contact VeriSign for professional support online or via telephone.
- Once the code is removed, you can have your site rescanned within 24 hours.
- If the scan is passed, the trust seal is displayed again automatically.

+ The Results

Trust equals more revenue. VeriSign seal users report transaction increases of from 10 to 36 percent with an average increase of 24 percent, in over 30 tests.*

Case Study: Web-based Law Firm Build Trust With Clients and Increases Sales with VeriSign Trust Seal

Company: The Trademark Company, one of the largest and fastest-growing trademark law firms in the United States

Challenge: To instill client trust in its Internet-based law firm web site; provide clear signs the company is legitimate; reduce-trust related questions and concerns from potential clients

Solution: VeriSign Trust Seal

Results:

- Boosted sales of key service packages by 40 percent and increased conversion rates by 15 percent
- Elimination of all email inquiries from potential clients

*Tests conducted using VeriSign Secured Seal

- about the legitimacy of its business
- Dramatic growth: the company is none of the top three trademark firms in the country

The Trademark Company was founded in 2003 by Matthew Swyers. His goal was to create a different kind of law firm where every client, regardless of size, has access to affordable, high-quality, trademark representation. To keep costs down, his unique approach was to offer trademark services online. Providing legal services online is still a rather radical idea. The biggest obstacle for Swyers and his team was to prove to visitors that his site was legitimate and trustworthy. The solution was to find a well-known brand with a strong reputation for online trust, which led him to VeriSign, the most widely recognized provider of online safety.

Results have been very good with significant increases in both conversion rates and sales. It is now one of the top three trademark law firms in the U.S.

When you consider that VeriSign delivers this sort of trustworthiness for \$299 a year, it's easy to see why the VeriSign seal is the #1 trust mark on the Internet.

+ Obtaining the VeriSign Trust Seal

Once you've decided you would like to register for the VeriSign Trust Seal, we will first verify the information you provide. Your web site must be legally registered and you must either own the domain name or have exclusive rights to use it. Next, we conduct your first malware scan. If malware is detected, you will receive a notice with details about the type of malware and the infected pages for removal. When you pass the malware scan, you'll receive an email alert with a link to a download page. VeriSign Trust Seal is a small script that you copy and paste into your Web site.

+ About VeriSign

VeriSign Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, VeriSign

helps companies and consumers all over the world engage in communications and commerce with confidence. Additional news and information about the company is available at www.verisign.com.

Visit us at www.Verisign.com for more information.

©2010 VeriSign, Inc. All rights reserved.

VeriSign, the VeriSign logo, the Checkmark Circle logo, other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

VeriSign, Inc.
2010-06-21

