WHITE PAPER:
GROW YOUR BUSINESS BY
BUILDING CUSTOMER TRUST

White Paper

Grow Your Business by Building Customer Trust

The Secret Ingredient of Internet Success

Symantec™

Norton™ SECURED
powered by VeriSign

Grow Your Business by Building Customer Trust

The Secret Ingredient of Internet Success

CONTENTS

Introduction

Building a successful small business website is a huge challenge. Whether the site is merely promotional or a full-service e-commerce enterprise, you – the small business 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 website and do business with me?
- Should I really worry about my website getting attached 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 who are attacking your customers.

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 is Where the Norton Secured Seal Comes In

The Norton Secured Seal can help build this sense of trust by bolstering security and authenticating your site. Why? Because the Norton Secured Seal is displayed up to 800 million times a day on more than 100,000 websites in 165 countries, and in search results on enabled browsers, on partner shopping sites, and in product review Web pages. In tests, 40 percent of consumers trust the Norton Secured Seal, more than our competitors' trust seals (U.S. Online Consumer Research, January 2011).

Consumer Trust is More Important than Ever Before

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.

- In 2010, Symantec encountered more than 286 million unique variants of malware (Symantec Internet Security Report, 2011)[1].
- 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009 (Symantec Internet Security Report, 2011)
- The total bill for cybercrime footed by online adults in 24 countries topped $388 billion over the past year (Norton Cybercrime Report, 2011)[2].

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 – and for a good reason. According to the 2011 Norton Cybercrime Report, victims of cybercrime spent 10 days on average trying to satisfactorily resolve cyber attacks.

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.

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 websites 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

[1]Source – http://www.symantec.com/business/threatreport/
[2]Source – http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

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 website. 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. 90 percent of respondents will not complete their purchase when a warning page pops up during a purchase, and 56 percent of respondents go to a competitor's website to complete their purchase in response to a security warning.[3]

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.

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 websites 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?

Building Trust Online

Consumers and business owners might not always full 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 trust seals a company can earn from third-party audits of site safety.

The Norton Secured Seal is the most recognized trust mark on the Internet:

- The Norton Secured Seal is displayed up to 800 million times a day.
- It appears on more than 100,000 websites in 165 countries.
- It also appears in search results on enabled browsers, partner shopping sites and product review Web pages.
- 77 percent of consumers recognized the Norton Secured Seal in tests, more than our competitor's trust seals.[4]

Displaying a trust seal significantly and positively influences consumers' willingness to buy the product or service offered on a website.

[3]Symantec U.S. Online Consumer Study, March 2011
[4]Symantec U.S. Online Consumer Research January 2011

The Customer Life Cycle

When it comes to running an online business, there is an ideal customer life cycle that all online retailers want to achieve. In tests, 94% of respondents are likely to continue an online purchase when they view the Norton Secured Seal during the checkout process, more than other seals or no seal displayed.[5]

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 website 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 Must be Established Quickly

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 links if they know a site is sophisticated enough to take security seriously, and that is not a phishing site, an imposter's counterfeit site, a virus delivery site, or a compromised legitimate site. Additionally, if you can establish trust ahead of time, you can drive more traffic to your website.

One benefit of the Norton Secured Seal is that it shows up as part of your listing on a search engine results page, thanks to our unique Seal-in-Search™ technology. This can make a real difference in producing more clicks to your website. When potential customers see search engine results, they can immediately identify websites that have been authenticated by Symantec.

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

[5]Symantec U.S. Online Consumer Study, March 2011

Trust at the Site Level

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

You can do this by displaying trust indicators that are:

- Clear and distinct
- Immediately recognized
- A reliable name or brand
- Hard-earned

Without Trust, You're Losing Money

There are some websites that are so well-known (e.g. Apple, Amazon, PayPal, eBay, and 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 online business is as reliable and safe as the larger, better-known online retailers.

What Happens if My Site's Security is Threatened?

Every day, Symantec 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, Symantec takes action immediately by:

- Sending you an automatic e-mail notification that malware has been detected on your site.
- Symantec next removes the seal from your site.
- The Symantec™ Trust Center will identify the infected files, tell you the location of the malware, and give you an actual view of the offending code.
- Symantec will also provide tips for removing the malware. If necessary, you can contact Symantec 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.

Obtaining the Norton Secured Seal

Once you've decided you would like to register for the Norton Secured Seal, we will first verify the information you provide. Your website 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. The Norton Secured Seal is represented in the email message as a small script that you copy and paste into your website.

More Information

Visit our website

http://go.symantec.com/trust-seal

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com