2015

EXPERT GUIDE

WEBSITE SECURITY

PROTECT YOUR WEBSITE. PROTECT YOUR MONEY.

www.trust-guard.com

WEBSITE SECURITY 101

Website security can be daunting, especially when you're a busy business owner who already has a lot of balls in the air. So we've put together this **free Website Security 101 Guide** to give you the basics on what you need to get secure and protect your site, your business and your livelihood.

2014 Was Just The Beginning Of A Decade Of Data Breach

It seems that writers were a little quick to name 2014, "The Year Of The Data Breach," as if were the only standalone year in digital chaos. This is our world now. Our entire lives are online so naturally the criminals are too. **We didn't peak in 2014: This is the decade of data breach.** Better yet, the millennia of data breach, because it's not a problem that will go away anytime soon.

Jay Johnson wrote for *Forbes* that, "Data breaches dominated headlines in 2014,…While the cybersecurity plights of certain high-profile retailers, financial institutions, and one prominent movie studio became common knowledge and headline fodder, these companies were far from the year's only victims. In fact, **a recent study found that more than 40% of companies experienced a data breach** of some sort in the past year – four out of ten companies that maintain your credit card numbers, social security numbers, health information, and other personal information. That number is staggering, and shows no signs of retreat."

Just five days into the New Year, headlines exploded with a possible security breach at Chick-Fil-A after the company noticed strange credit card activity in a number of restaurants. In a recent statement they said:

"We want to assure our customers we are working hard to investigate these events and will share additional facts as we are able to do so. If the investigation reveals that a breach has occurred, customers will not be liable for any fraudulent charges to their accounts — any fraudulent charges will be the responsibility of either Chick-fil-A or the bank that issued the card. If our customers are impacted, we will arrange for free identity protection services, including credit monitoring."

Since 2014 was the first year of real security breach, a glimpse into our future for years to come, it finally reset the bar for security standards. Unfortunately it took thousands of security breaches last year, and countless victims, to inspire lawmakers, business owners, and customers to take security seriously. 2014, if anything, has set a precedent to prevent and

quickly handle security breach for businesses. 2014's security breaches reminded politicians and lawmakers of the new era of data breach, and educated customers that things that are out of site, such as digital information, is not necessarily out of mind.

4 Expert Ways to Thwart Hackers

Alarming newspaper and industry reports show that no one, including small businesses, is immune from a potential data security breach. According to a 2013 survey by National Small Business Association, half of all small businesses surveyed had been a victim of a cyber attack.

The best way to protect yourself is with a comprehensive security protection plan and knowing some of the tricks hackers use that can cost you time, money and spur mistrust from your customers. Here are four risks that could make you a target for hackers – and how you can fix them.

Risk: Weak passwords

The necessity of a strong password is so basic it should be a no-brainer, right? But a strong password is one of your first lines of defense against unscrupulous hackers, so it bears a mention.

Fast Fact: Studies have shown that website users typically have only one password for multiple accounts, leaving customer information and business data vulnerable to hacking.

What you can do: Experts recommend you create a password that's at least eight characters long, with a combination of capital letters and symbols. And it's better if passwords aren't real words, either, which makes them easier to hack. Create a password that's gobbledygook (that you can remember) rather than a real word and you're more likely to evade hackers.

Risk: Phishing

We've all gotten those emails: an African prince needs us to transfer him money, etc., etc. Some attempts to steal our data and get our money are so blatant it's almost laughable. But there are more subtle phishing techniques out there, that, if you're not vigilant, could be as simple as one unaware-click away to open the door to a hacking maelstrom. Phishing can come in the form of a legitimate-looking email with an attachment or link to a virus, malware or spyware.

Fast Fact: Phishing attacks have been steadily rising each year, according to the Anti-Phishing Working Group, which works to create a unified global response to cyber crimes.

What you can do: Don't click without thinking first. Copy and paste a link to a URL rather than clicking on it. Keep your operating system and software up to date.

Risk: Untrained staff

You can have an exemplar internet security plan in place, but have your employees been trained on how not to let an intruder in through the gates? Employees not trained on cyber security methods is like having staff who don't know how to set the code for the alarm system.

Fast Fact: Nearly 19 percent of Americans surveyed said they had never changed their PIN or password without first being prompted, according to a survey conducted by The National Cyber Security Alliance and PayPal.

What you can do: The National Cyber Security Alliance, a nonprofit focused on internet safety, recommends training employees to create strong passwords, to back up their work and how to spot and not click on suspicious links and attachments in emails.

Risk: Social engineering

Instead of tediously trying to hack into software, hackers try to get information directly from the source: you. They may try to get you or an employee to install malicious software or use you to gain access to unauthorized locations.

Social engineering is one of the latest tactics hackers use and is on the rise, according to a January 2014 recent article from Inc. Magazine.

Fast Fact: The average cost to a small business that's been hit by a cyber attack was more than $9,000, according to a 2013 National Small Business Association survey.

What you can do: Be careful of what personal information you reveal online. Beware of hackers pretending to be from your company's IT department and asking for sensitive data or passwords.

6 Key Security Terms You Need to Know to Protect Your Site

If you're a business owner trying to make sure your website is safe, secure and trustworthy to customers, navigating your way through the dizzying array of cyber security-related can be confusing, frustrating and just plain boring. We've put together this in-a-nutshell guide to make it as painless and simple for you to understand some key terms so you know what your site needs and why.

Trust Seal

What it is: Trust Seals are graphics for your website's homepage that show customers your site is safe and secure and that you are who you say you are. There are many companies that offer various kinds of trust seals. The three main types are Privacy Seals, which lets customers know their personal and financial information is safe; Business Seals, which show that an outside company has verified that you are who you say you are; and Security Seals, which demonstrate that your site has been scanned for viruses and security holes.

Why you need it: More customers, more sales, more ka-ching! Trust seals have been shown to increase consumer confidence, decrease shopping cart abandonment and boost sales. When customers feel your site is secure, they're more likely to buy from you. Trust Guard offers three types of trust seals to meet your site's individual needs.

Privacy Policy

What it is: A privacy policy lets visitors know what information you collect from them and what you do with it. In legal terms, a privacy policy is a disclosure document. There are state and federal laws governing internet privacy and the FTC and state attorney generals have jurisdiction in enforcing those laws.

Why you need it: A comprehensive, specific privacy policy tailored for your site can help protect you against complaints and potential lawsuits. Facebook and Google have each faced lawsuits connected to their privacy policies and use of user data. But be aware that simply copying and pasting an existing privacy policy from another company's website simply won't do: you need one that matches the specific ways in which your company gathers and uses visitor information. Many companies, such as Trustee and FreePrivacyPolicy.com, offer services to create privacy policies for your site in minutes.

SSL Certificate

What it is: An SSL (it stands for Secure Sockets Layer, if you really want to know) Certificate is a digital form issued by an outside party that says your site is authentic and uses SSL encryption. SSL encryption scrambles data from a customer's computer to your server so their info is protected from third parties trying to access it. SSL certificates include the certificate holder's name, the certificate's serial number and expiration date, a copy of the certificate holder's public key, and the digital signature of the certificate-issuing authority.

Why you need it: If your company takes online payments or collects sensitive information, you need it. An SSL certificate is an added layer of protection to help assure your customers that your website is safe. It won't protect you (or them) from hackers, but when visitors see the padlock in the browser window that indicates that SSL encryption is being used, it can help build confidence that your company is taking steps to protect their data.

PCI Compliance

What it is: Payment Card Industry Compliance applies to you your company collects, transmits, processes or stores cardholder information. Being PCI Compliant means you're following industry requirements to keep your customers' data safe. The regulations were developed by a council (Payment Card Industry Security Standards Council - aka PCI SSC) set up by the big credit card companies - Mastercard, Visa, American Express, Discover and JCB.

Why you need it: Do you want to pay massive fines? Didn't think so. If you're not PCI Compliant, then you've got to pay up. The regulations are too complex to get into in a brief summary, but we've got the lowdown for you here.

Vulnerability Scan

What it is: Vulnerability Scans check for security holes in computer networks to make sure you're not letting the bad guys in. They typically are automated scans and should be run continuously.

Why you need it: You don't want hackers stealing your info, causing your customers to distrust you and costing you money, do you? Of course not! Vulnerability Scans help protect your network and your customers' data and are the first step toward being PCI Compliant and getting a Trust Seal (we mention both above.) For more details on vulnerability scans, we've got it covered here.

IT Penetration Test (PenTest)

What it is: PenTests actively, intentionally attack and exploit a computer system to see if there are any holes in your network. It's basically like a hacker attacking your network, only they're on your side. PenTests require expertise and aren't automated like vulnerability scans are.

Why you need it: Combined with vulnerability scanning, Pen Tests give you comprehensive security coverage. PenTests should be done once a year by a computer security expert (or good guy hacker, if you will) to identify what data was compromised during the test. Need more on Penetration Testing? You can find it here.