THE NATIONAL CYBERSECURITY SOCIETY

How To Set Up A Secure Website

INTRODUCTION

You are a small business owner and YOU WANT TO REACH MORE CUSTOMERS but that depends on your connectivity to the Internet.

You want to pay and be paid on time, through automated transactions but you are worried it won't be secure.

Are you confused about how to set up on-line transactions safely and securely?

We are here to help!

RESOURCES NEEDED

Hosting Services - A secure website - where your company website is hosted | SSL/TLS Encryption | Back up and Restore
DNS Protection | Secure Password | Staff Assigned | Employees Trained

STEP-BY-STEP INSTRUCTIONS

1. *Select a Hosting Service*

Unless you're a technology security company, we don't recommend you host your website on your company or home server.

Recommendation: Buy website hosting services from a commercial service provider. There are many available. Ensure the company can support SSL/TLS encryption, security monitoring, and a back up copy of your website.

Commercial Website hosting companies have the ability to provide:

- Availability – nearly 99.99% availability - meaning you're always open for business!
- Flexibility – ability to expand when your business grows
- Security – up to date security monitoring and patches aligned with industry standards
- Data Backups – your website and website content will be backed up – another way to ensure you're always open for business!

2. *Select SSL/TLS Encryption*

SSL/TLS are protocols used for encrypting information between two points. SSL Certificates are issued between the two entities, usually between server and client, but there are times when server-server and client-client encryption are needed.

By selecting the feature of SSL/TLS encryption, your company and customer's private information such as passwords, credit card numbers are encrypted. What that means, if someone were to hijack the data transmission the data would be encrypted and the bad guys won't be able to steal it or read it. Without this feature, your data is transmitted in the clear, and anyone can read it, steal it or manipulate it.

Customers can buy with confidence, knowing their info is safe, and your website URL will have the https:// qualifier, meaning their web experience will be safe.

Recommendation: Buy website hosting services from a commercial service provider that provide the ability to encrypt data (SSL/TLS) and purchase the SSL certificates.

3. *Select Backups and Restore*

Most hosting companies provide a backup copy of your website content and the ability to restore your site to an earlier version if you get into trouble. This is usually a standard feature – but we want you to check and make sure you select a plan that provides you this flexibility.

Recommendation: Select a hosting service that guarantees website back up and restoration services. Ask how long it will take for them to restore your site to an earlier version. If you can be down for a day or two, then at least you will know in advance. If you can't be down for a day or two, select a service provider who can restore your site within your time constraints to keep you in business.

A site down, means no business and this affects your reputation!

It's always important to know your plan's features in advance!

Write it down and keep restoration information in your back up plans!

STEP-BY-STEP INSTRUCTIONS

4. *Select DNS Protection (DNSSEC)*

This is a premium service, but well worth the cost. Ever wonder if a hacker could interfere with your site and redirect users to a site that looks just like your site, but they steal all of your customers and business? Domain Name Server (DNS) converts your URL (www.howtoguide.com) to a series of numbers (an IP address) that a browser uses to locate a website. When you type a domain name into your browser, the DNS looks through a huge database to find the right IP address you requested and directs your browser to the correct website content. DNSSEC or DNS Security stops hackers by securing the look up process and verifying the visitor is actually arriving at your site.

RECOMMENDATION: Select DNSSEC as a service with your website hosting contract. This will improve performance, accessibility and security by placing you DNS information in a secure location. The hosting company will place your DNS information in multiple servers around the world, so visitors searching for your site can get connect to the closest server location for a faster response.
It eliminates the error, "website not found", which usually happens when a server is slow to respond.

With this feature, hackers won't be able to redirect your customers to their website to steal user names, passwords or credit cards numbers.

5. *Select a Secure Password*

When you establish a website account, you will be asked for a user name and password. Simple right? Not so simple, your password shouldn't be password! Ever wonder how to come up with a good password? And what other tips should I keep in mind. Passwords should be at least 10-12 characters in length. The longer the better! Here are some easy tips.

Pick two words that don't go together, add a capital with lower case letters, add some numbers and special characters within the string…

Here are some suggestions:

- **Busy3$%mom**, *not busy1234bee*
- **Small3*$#trainor**, *not Small1234business*

And change your password regularly

6. *Assign a Staff Member – As Website Owner*

Having a website owner or "system owner" is one of the critical steps in managing a website or any critical system or service. He/or she can manage the account, keep up to date on the latest changes, interface with the website hosting company. He/she should keep up to date records of changes made to the website, contract details, restoration details, etc. He/she is the go-to person for keeping the website up and operational and interfacing with the hosting provider. This can be a part-time job, but because it is such a critical function for your on-line business and reputation, it's important to have the responsibility defined and assigned.

RECOMMENDATION: Assign a member of your staff as the website or system owner and assign him/her duties of keeping up-to-date records of the website changes and content.

7. *Train Employees*

Are you wondering why training is listed in setting up a website? Employees need to understand the value of protecting customer data, and to stay watchful and speak up. Customers who call in and need help navigating the company website, employees need to take care in the information that is given over the phone. Employees should not be writing down customer credit card data – but rather instruct the caller on how to enter this information on line.

Another key tip with the website related to employee training, is to instruct your employees to be watchful and speak up. Have they noticed that the website content has changed? Did they ask the website owner (item #6) whether there was a recent change in content?

RECOMMENDATION: At least every quarter, remind/train employees on how to protect customer data, and to stay watchful and speak up. In most cases, your employees can be your first line of defense!