THE NATIONAL CYBERSECURITY SOCIETY

HOW TO SECURE YOUR WEBSITE

DID YOU KNOW?

- ✓ Compromised websites are used for a number of reasons:

  – To redirect traffic to a hacker's spurious website; steal customer data including payment and email information; host malware, spam pages, and/or porn; advertise illicit products; or simply vandalize the site.

- ✓ Ransomware, a type of malware, has become the latest threat to the business community - whereby criminals lock or vandalize the website and demand a ransom before the website can be put back into use.

- ✓ Having an unsecure site offers criminals the platform to launch these crimes.

Your reputation depends on securely connecting to your customers and suppliers via the Internet. Do you know how to create a secure website?

STEP 1: HOSTING SERVICE

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

Purchase 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
- 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 are resilient

STEP 2: 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.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Secure Website continued…

STEP 3: BACKUP

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 check the plan to ensure you have this provision.

Ask how long it will take 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.

STEP 5: DNS SECURITY

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.

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 connected 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.

STEP 6: ESTABLISH A LOGIN/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! Passwords should be between 10-20 characters – the longer the password, the harder it is for someone to crack.

- Don't use words or phases that link to who you are, where you have lived – street, city you were born, date you were married, your business name, your business owner, kid's names or birthdays.
- Change your password every three months or when prompted by the hosting provider
- The password you established should only be used for your website, don't reuse passwords.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Secure Website continued...

STEP 7: ASSIGN AN 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, and interface with the website hosting company. He/she is responsible for keeping 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 online business and reputation, it's important to have the responsibility defined and assigned.

STEP 8: TRAIN

Training employees is a critical step in ensuring your site is functional and resilient. Your employees can be the first line of defense – by knowing your website, and whether it's functioning as it should. They need to be advised they should notify your website "system owner" and website hosting provider if the site is not functioning as it is intended.

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 could actually be hackers trying to steal critical data. Employees need to be trained not to give out critical information over the phone. Employees should also be advised not to write down customer credit card data – but rather instruct the caller on how to enter the information on line.

At least every quarter remind/train employees on how to protect customer data, and to stay watchful of your critical asset – your website.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.