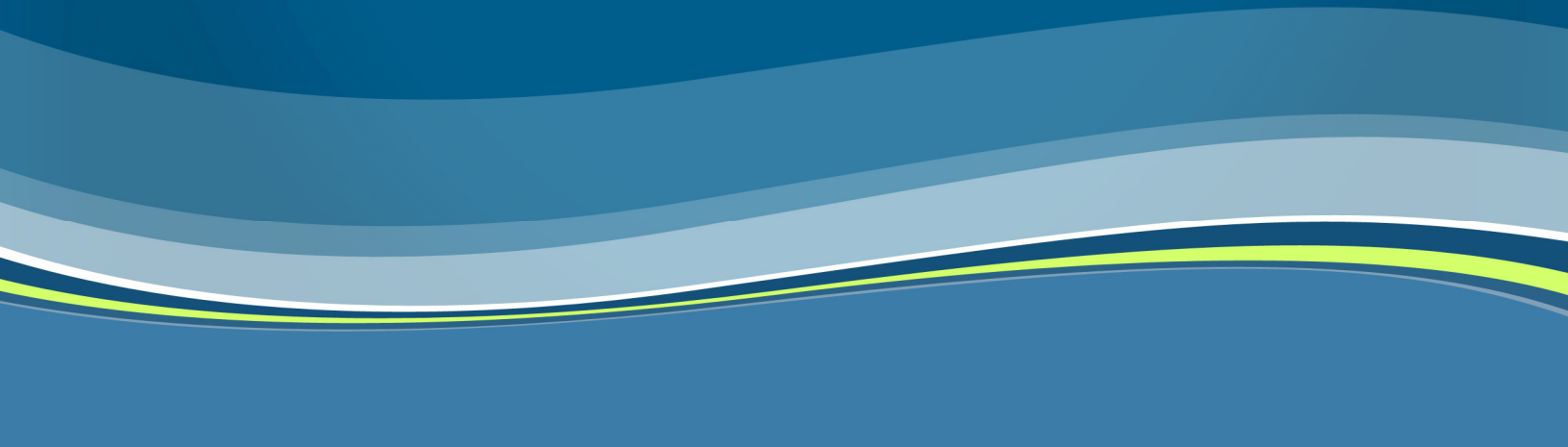


NetworkSolutions®

Web Presence Security



Network Solutions® is a leading provider of Web solutions that help small businesses find success online.

Getting your business online is about reaching out and connecting with millions of potential customers, buyers, and partners. Building a Web site is the most scalable way to attract potential customers from all over the world. Simply put, a Web presence expands your market significantly and instantaneously. **The following steps are essential in creating a complete Web presence for your business:**

- Choose a Domain name (i.e. your Web site's name).
- Set-up an E-mail address for your Web site.
- Create a Web site (there are several different kinds and many ways to do this)
- Make it secure (security protects your customers' data when it is transmitted between their computer to your site.)
- Get your Web site found (by creating an online marketing plan)

What is Web Presence Security?

Web presence security means that your Web site:

- Is free from vulnerabilities that identity thieves can exploit.
- Does not contain malicious programs installed by hackers.
- Is available and performing as designed and as needed by your visitors.
- Is authenticated as a legitimate Web site to prevent phishing, fraud, or scams.
- Encrypts all sensitive data transmitted between the site and a visitor.

To ensure that your Web site is safe and available for your customers to visit, you need to monitor your site for vulnerabilities and performance using a Web site scanning service like [Network Solutions WatchDog™ service](#).

If your business or organization communicates or collects any kind of sensitive information or conducts transactions via the Internet, the data that is transmitted between you and your customers should be protected by an SSL Certificate like those offered by [Network Solutions SiteSafe™ service](#)

Why do you need Web Presence Security?

Web presence security is in many ways the most important aspect of online business – both for you and for your customers. Web presence security is both a business *protector* and a business *enabler*.

Numerous government and industry regulations require that you protect your customers' online activities and report any breaches of your customers' data; failure to do so can result in penalties, fines, or even prosecution.

In 2006, approximately \$913 million in e-commerce sales were lost because of security concerns among online shoppers (Gartner Survey, August 2006 <http://www.gartner.com/it/page.jsp?id=498974>).

Therefore, it is not only imperative that you ensure your Web presence is protected, but that you assure your customers of that fact through "secure site seals" and other indicators that inspire the confidence they need to know your site is safe to handle their business. This

trust will enable you to convert your site's visitors into customers.

What are Web Site Scanning Services?

Web site scanning services, like [Network Solutions WatchDog™ service](#), will continuously scan your Web site to detect vulnerabilities and monitor performance. These services will alert you to any vulnerabilities or performance problems that are detected so you can address them immediately.

Thousands of known vulnerabilities exist that both hackers and identity thieves look for on a Web site resulting in new vulnerabilities every day. Once found, these vulnerabilities can be exploited. Luckily, there are patches available to fix most security breaches once you are aware of them, and these scanning services provide detailed instructions to help you protect your site from hackers.

Web site scanning services monitor your site's performance (page load times and availability) by accessing your site every few minutes from various locations around the world. If your site is not available or is loading too slowly, the service will alert you so you can contact your hosting provider to address the problem. Performance problems can be the result of "denial of service" attacks by hackers, or can be caused by hardware failures or bandwidth limitations at your hosting provider. Regardless of the cause, your Web presence must be available for it to be an effective business tool.

Signs of Secure Sites

Vulnerability scanning services like Network Solutions WatchDog will provide certification

seals to place on secured Web sites to indicate to visitors that this site has passed its latest security scan and is safe. These certification seals will contain information about the company and the date of the most recent scan that was successfully completed. Security certification seals help customers feel more confident when visiting your site or making online transactions.



What are SSL Certificates?

Secure Sockets Layer (SSL) Certificates assure you and your customers that the transactional information (names, addresses, payment information, etc.) entered on your Web site is encrypted, private, and protected.

SSL certificates are issued by Certificate Authorities (CA) which are third-party organizations that authorize and endorse the legitimacy of Web sites. The actual certificate itself contains information about the owners of the Web site and the Certificate Authority that issued the certificate. Internet browsers like Internet Explorer, Firefox or Opera are set-up to trust an SSL certificate if it is current and is issued by a reputable CA. A properly acquired and installed SSL confirms the legitimacy of your site and its ownership, as well as the security of the connection established between your site and your customer's browser.

There are three types of SSL Certificates, which are categorized by the rigor of the validation process that went into the investigation by the certificate authority. Depending on the level of security and authentication you require, you

can choose from Domain Validated, Organization Ally Validated, or Extended Validation. Each level of SSL requires a different type of authentication and comes with different features.

There are three main CA Validated Certificates:

Domain Validated (DV) Certificates:

This validation procedure is the least rigorous; the CA checks only that the applicant's name and contact information matches the registration information in the WHOIS database for the domain name associated with the SSL Certificate. DV Certificates are a good choice for businesses collecting non-financial information, intranets or extranets.

Organizationally Validated (OV) Certificates:

An OV Certificate is issued only after verifying the legitimacy of the applicant's business. That verification includes checking business credentials (e.g. Articles of Incorporation) as well as the legitimacy of the business' Web and physical addresses. For businesses accepting credit-cards and processing other sensitive information, OV Certificates are a good choice.

Extended Validation (EV) Certificates:

The most rigorous validation process employs industry-wide standards established by leading CAs and browser developers. EV Certificates are available to all business and government entities, but are not available to individuals. EV certificates are ideal for businesses that conduct high dollar or high volume monetary transactions, collect highly sensitive information subject to regulatory scrutiny, and that want an additional visual indicator to help establish trust with customers.

Depending on what information your Web site collects from your customers, you should take steps to ensure the privacy and security of your visitors.

Signs of SSL Security

A site that is protected by an SSL Certificate provides visual indications to you and your customers that security has been established and that it is safe to transact. The common indicators include the locked padlock symbol as seen here:



the "https" prefix in the browser address bar.

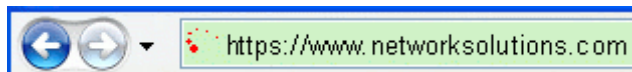
A site Seal that, when clicked on, provides information confirming the authorized status of the site in question.



Certificate Authorities typically offer site Seals with their Certificates as visual symbols assuring that the site and transactions are protected and secure. Businesses display these symbols prominently on their Web sites to promote the fact that their site is validated and safe.

For organizations that do not need to sell or transact online, some CAs offer a stand-alone “site Confirm Seal”. This site Confirm Seal validates a Web site to show it is a legitimate business but does not include encryption capabilities.

The final and newest visual indicator is only available with Extended Validation SSL certificates. With an EV in place, the browser navigation bar in Internet Explorer® 7 and Firefox 3.0 turns green. This highly visible security indicator provides added assurance that your site is secure and that you are a legitimate business.



SSL Certificates are a simple, affordable and smart way to provide enhanced security and outside verification of a Web site’s security. Additional benefits include increased customer confidence, compliance with regulatory requirements (higher conversion rates??), extra protection for your business reputation, and defense against possible penalties and criminal prosecution.

Prerequisites for Security

You will need your domain name and Web site to begin the process of setting up security for your business. Depending on the kind of certificate you need, you will also need to submit information to the Certificate Authority about your business. The process can take time so plan ahead and get started getting the certificate you need.

Now that you know the essentials of Web site security, you are ready to learn about online marketing and what you need to know in order to help your customers find you online.