

NetNames Security

If your website captures any visitor data such as contact or payment details, you should ensure that the information is safe and that your customers can be confident of your online security levels. This type of security can be achieved through the use of a combination of online security tools:

- Secure Sockets Layer (SSL) Certificates
- Trust Seals
- Premium DNS Security
- DNSSEC

To assist you in organising adequate levels of online security for your company, NetNames can provide any of the above tools for your domain names and websites.

According to recent surveys:

- 80% of online shoppers want more assurance that their information is secure ⁽ⁱ⁾
- 87% of online shoppers are familiar with website security ⁽ⁱⁱ⁾
- As many as 40,000 websites are compromised per week ⁽ⁱⁱⁱ⁾



Find out how to protect your brand online at www.netnames.com

NetNames Security

SSL Certificates

When information travels across online networks without SSL encryption, that data can be intercepted by potential identity thieves or fraudsters. Secure Sockets Layer (SSL) Certificates are used to encrypt data and authenticate parties, so that only those authorised are able to access and make use of the data.

An SSL Certificate is typically created for a particular server in a specific domain and is verified against a particular business entity. It acts like a passport or a driving licence and can only be issued by a trusted Certificate Authority (such as VeriSign), which performs identity checks to the required level for each Certificate.

How do SSL Certificates work?

SSL Certificates work by using a public key to encrypt information and a private key to decipher it. When a browser points to a secured domain, an SSL handshake happens between the server and the client, and establishes both an encryption method and creates a unique session key, which is used to encrypt message data between the two parties. The user can then begin a secure session that guarantees message integrity.

If you do not already have SSLs for your e-commerce websites, NetNames can provide you with a number of different options:

- **Domain Validated (DV) SSL Certificates:** The Certificate Authority authenticates the right of the applicant to use a specific domain. Corporate information is not vetted or displayed on the Certificate
- **Organisation Validated (OV) Certificates:** The Certificate Authority conducts some organisational vetting as well as verifying the right of the applicant to use a specific domain. Company information is displayed on the Certificate
- **Extended Validation (EV) Certificates:** The Certificate Authority undertakes an extensive vetting of the applicant organisation including verifying the legal, physical and operational existence of the entity, matching the entity with official records, confirming that the applicant has exclusive rights to use the domain and verifying that the real applicant has authorised the issuance of the Certificate

Free SSL Certificate audit

NetNames can check the status of your SSL Certificates by offering you a no obligation SSL Certificate audit to highlight:

- The number of SSL Certificates on your websites (on external sites only)
- Current providers of your SSL Certificates
- The expiration date of your SSL Certificates

If you would like to know more information about commissioning a free audit of your Certificates please contact NetNames.

DNS Security

The Domain Name System (DNS) is vital for directing not only website traffic to the right place, but also email to the correct inboxes. As such, a failure in the DNS has the potential to eradicate your entire online business presence from the world wide web as well as bringing your email and e-commerce capabilities to a halt.

Organisations cannot afford to have their online presence unavailable for any length of time. It is therefore imperative that businesses choose a domain registrar that uses a robust, highly available and sufficiently secure and robust DNS infrastructure.

NetNames can provide you with access to one of the world's largest DNS networks, giving you a robust defence against outage threats – as well as offering rapid query response rates.

This extensive mesh of 16 synchronised DNS server nodes, distributed across six continents, provides NetNames' clients with unprecedented levels of performance and resilience. It also provides the reassurance of knowing your website addresses are hosted on a resilient network of servers located in multiple data centres, offering ultra fast delivery of mail and web content regardless of where your users or customers are based.

DNSSEC

When the current DNS architecture was originally deployed in 1983 the focus was on ensuring scalability and distributed management, security was a secondary concern. Over the years security of the DNS infrastructure has become increasingly important as a number of high profile incidents have come to light.

In 2003 the United States Government highlighted the DNS system as one of the key weaknesses in its 'National Strategy to Secure Cyberspace' whitepaper. This led to the development of a number of security propositions concerning the DNS infrastructure, one of them being DNSSEC.

DNSSEC stands for 'Domain Name System Security Extensions'. Its intent is to protect Internet users from 'cache poisoning' attacks. In these DNS attacks the Internet user, whilst clicking on a hyperlink, is diverted to a rogue IP address.

In July 2010 the domain name system's root zone was digitally signed, placing DNSSEC at the top of the DNS hierarchy. .Com was also recently signed along with other major TLDs. The signing is significant because it means that when an individual types in a domain name (such as example.com), they are able to trust the domain name because they trust the root zone.

How will DNSSEC improve online security?

In simple terms DNSSEC will ensure that the data on IP addresses and domain names comes from a verified source, putting an end to redirection attacks. Effectively, the integrity of the DNS will be ensured because the data served by each server in the DNS hierarchy will be digitally signed. A name server or client resolving a name can therefore check the integrity of the data at each level i.e. root, .com, example.com, www.example.com. If it does not get the correctly signed response then it will not make the connection.

Currently a small number of registries have already adopted the DNSSEC security extensions and NetNames will support DNSSEC for any TLDs which use it now and in the future.

Trust Seals

Whilst SSL Certificates can underpin the security of online transactions, they cannot give assurance to your customers that the branded goods they purchase online are genuine products from your organisation or your authorised resellers. Trust Seals can do this however, and should therefore be factored into the overall security needs for your website(s).

What are Trust Seals?

If your organisation conducts business and transactions with your customers online (either via your own websites or through the websites of authorised resellers) you will know that the amount of confidence that consumers have in the website(s), is the overriding factor in whether a consumer will purchase your goods or not.

Trust Seals can help build this confidence as they are a visible means of authenticating that the goods sold online are legitimate, or that the owner of the website has been authorised by you – the brand owner – to sell your products or services.

When a Trust Seal is displayed on a website, it means that both the brand owner and a trusted third party have verified the business or individual identity of the website. (Visitors may also click on the seal to confirm the information.) The Trust Seal also means that the website has passed a daily malware scan to encourage visitors to click on the website with confidence.

Trust Seals can be provided as part of an SSL package or as stand-alone privacy seals or business seals for your websites.

For more information about Trust Seals, please contact us today.

Trust Seals bring trust to resellers, distributors and affiliate businesses by helping them establish credibility online.

NetNames Security

" We posted the VeriSign Secured Seal on the payment pages and found that completed sales rose by approximately 10% in comparison to the previous week's results. "

Warren Jonas, Head of Service Management, Opodo

NETNAMES UK

Prospero House
241 Borough High Street
London SE1 1GA

UK

Tel: +44 207 015 9200
Fax: +44 207 015 9365
Eml: enquiries@netnames.com

Betjeman House
104 Hills Road
Cambridge CB2 1LQ

UK

Tel: +44 1223 372 400
Fax: +44 1223 372 401
Eml: enquiries@netnames.com

NETNAMES FRANCE

Green Side - BP 296
400 Avenue Roumanille
06906 Sophia Antipolis Cedex
France

Tel: +33 497 212 212
Fax: +33 497 212 211
Eml: enquiries@netnames.com

124-126 rue de Provence
75008 Paris
France

Tel: +33 1 48 01 83 60
Fax: +33 1 48 01 67 73
Eml: enquiries@netnames.com

NETNAMES USA

55 Broad Street
11th Floor
New York
NY 10004
USA

Tel: +1 212 627 4599
Fax: +1 212 627 5744
Eml: enquiries@netnames.com

NETNAMES GERMANY

Landshuter Allee 12-14
4. OG Nord
80637 München
Germany

Tel: +49 89 20 400 78 0
Fax: +49 89 20 400 78 10
Eml: enquiries@netnames.com

NETNAMES SWITZERLAND

Staffelstrasse 10
CH-8045 Zürich
Switzerland

Tel: +41 44 204 16 80
Fax: +41 44 204 16 81
Eml: enquiries@netnames.com

NETNAMES NORWAY

Majorstuhuset
Kirkeveien 64 A
N - 0364 Oslo
Norway

Tel: +47 21 54 98 00
Fax: +47 21 54 98 09
Eml: enquiries@netnames.com

NETNAMES SWEDEN

Mäster Samuelsgatan 60
111 21 Stockholm
Sweden

Tel: +46 850 516 472
Fax: +46 850 516 410
Eml: enquiries@netnames.com

NETNAMES DENMARK

Arne Jacobsens Allé 15
2300 København S
Denmark

Tel: +45 33 88 63 00
Fax: +45 33 88 61 01
Eml: enquiries@netnames.com