11
November
2009

This Issue

Recent DigiCert Clients

Cisco Technology, Inc.

Browning Arms Company

National Football League

TiVo Brands, LLC

AmerisourceBergin Corp

Software People A/S

Swiss International Airlines AG

visitthecapitol.gov

Telcommunications and Information Administration

Sallie Mae, Inc.

World Book, inc.

Cineplex World Entertainment Limited Partnership

New York State Office for Technology

Blistex, Inc.

digicert®

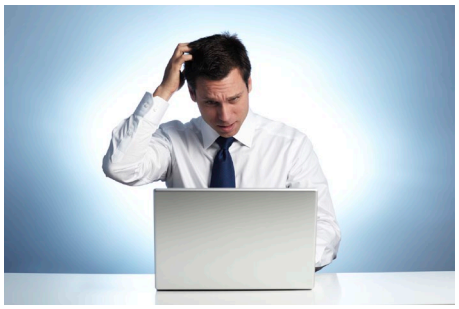
Your Success is Built on Trust™

What's In a Name?

Internal Network Name Best Practices

Choosing your Active Directory Namespace or your internal network name is a critical step in securing your organization's network. Your network name can drastically affect security as well as your ability to configure your network services and troubleshoot potential problems.

In order to minimize confusion or naming conflicts, there are two recommended practices for a naming structure.



1) Register a fully-qualified domain name to be used exclusively for internal sites and services.

If your organization's primary domain name is mycompany.com, a separate domain name, for example, mc.com, can be registered and used internally exclusively by your organization. Registering the name prevents other organizations from being able to also register the name and use it on their internal network. It also prevents confusion within your network by having your users access the external Web site of the organization that actually owns the domain name being used internally.

2) Make a sub-domain of your publicly registered domain name reserved for internal network sites and services.

Utilizing your primary domain name that is well known to your organization's users, you can also reserve a subdomain to be used for all internal Web sites and services. Each site or service used only internally within your organization would then be part of the same internal sub-domain.

Continued on Page 2

Win an XBOX 360 or Wii

Win a Nintendo Wii or Microsoft XBOX 360 Arcade from DigiCert just in time for the holidays! To be eligible, you must be a DigiCert customer and participate in our survey found at http://www.digicert.com/survey.php. Please give us your honest opinions and be sure to include your contact information.

Winners will be chosen at random and notified on December 10th, 2009. Terms and Conditions can be found at https://www.digicert.com/survey-drawing-terms.txt.

Private WHOIS Records

A Double-Edged Sword

By: Travis Tidball, Director of Customer Relations

Domain registration is a foundational requirement of the modern-day Internet - without a method to clearly identify ownership of domains, navigating to a specific site would most likely be an exercise of luck and patience.

It is generally accepted that the registrant, as shown on a domain's WHOIS record, is considered the domain's owner -- regardless of who purchased it. There have been instances where an employee registered a domain in their own name instead of their employer, leading to costly legal issues down the road.

Indeed, maintaining accurate Whois record information is important enough that The Internet Corporation for Assigned Names and Numbers (ICANN) requires annual reminders for an accurate Whois record.

"At least annually, a registrar must present to the registrant the current Whois information, and remind the registrant that provision of false Whois information can be grounds for cancellation of their domain name registration."

More information about ICANN's Whois Data Reminder Policy can be found at http://www.icann.org/en/registrars/wdrp.htm) With rising concerns of privacy and spam, some domain owners have opted to privatize or "mask" WHOIS record details.

"For fastest certificate issuance, ensure your WHOIS record is publicly visible."

To protect domain owners from fraud, DigiCert will never issue a certificate to an organization that does not own the domain or have permission to use it.

For fastest certificate issuance, ensure your WHOIS record is publicly visible - at least briefly while we validate your order.

"What's In a Name?" Cont.

by Flavio Martins, Director of Support & Validation

The DNS resolution for your domain name would then be set up as:

www.mycompany.com → Public IP Address
webmail.mycompany.com → Public IP Address
internal.mycompany.com → Internal IP Address
mail.internal.mycompany.com → Internal IP Address

These naming practices focus on reducing confusion within the organization regarding which names are external and internal, and also prevent the conflict of utilizing a domain name that is already owned by another organization.

Call us toll free (Canada or US) at 1-800-896-7973 (international Customers please call us at +1-801-877-2100). Visit us online at www.digicert.com (24-hour Live Chat service provided).

Browsers Patch Due to Null Attack Concerns

By: Travis Tidball, Director of Customer Relations

A recent phishing attack against PayPal users may have put extra pressure on Browsers to patch their software against Null Character SSL threats.

Both Internet Explorer and Safari were vulnerable at the time of the attack and have since released patches.

More details about Null Character threats can be found in the October 2009 edition of the DigiCert Newsletter - http://www.digicert.com/newsletters/DigiCert-Newsletter-2009-10.pdf

Checks were already in place to ensure that certificates of this type never have been, nor will be, issued by DigiCert.

Feel free to contact our Support & Validation staff at 1-800-896-7973 if you have any questions or want to report another example of this attack.

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com