

Reducing Domain Vulnerability Best Practices for Corporate Domain Name Management

Domain names are critical corporate assets that encompass your brands, trademarks, products and corporate identity. They protect your intellectual property on the Internet and enable your customers, partners and stakeholders to do business with you online.

Securing your intellectual property on the Internet entails more than registering and renewing your corporate domain names.

For starters: Does your organization know how to reduce its vulnerability to domain hijacking? Do you have a policy addressing access and administration privileges for your domain portfolio? Have you critically evaluated the security of your provider's DNS infrastructure? What recourse will you take if a name that represents your intellectual property is registered by another party or competitor?

To effectively manage a corporate domain portfolio, domain administrators need to be able to answer the above questions and more. To avoid problems and reduce domain vulnerability, organizations, corporations and government agencies need to strategically manage access privileges, administration duties, compliance requirements, acquisition procedures and the security of their domain name portfolio(s). Webnames.ca can help you put these crucial steps in place.

- Ensure all your corporate domain names are registered at one registrar and under a single master account
- Make use of a dedicated representative to help you manage your registrations, renewals, transfers and consolidation
- Ensure all your corporate domain names are registered in your organization's name and not that of an individual employee or administrator
- Assign one person within your organization to conduct your domain name registrations (Administrative Contact)
- Determine who, and under what circumstances, should have access to your account in addition to the administrative contact. Name a secondary point-of-contact in the event your administrative contact is not available and/or leaves your company
- Make use of Parent-Child account functionality if you want to grant a third party access to a specific domain name in your portfolio

Reducing Domain Vulnerability

Best Practices for Corporate Domain Name Management | page 2

- Use a provider with DNS redundancy added physical redundancy will protect your website(s) from DNS failure, traffic surges and potential human error
- Establish an internal domain transfer procedure outline who is responsible for initiating domain transfers as well as confirming transfer requests
- Use a domain registrar that supports and gives you directs “domain lock” (also sometimes called “registrar lock”) to prevent unauthorized transfers
- Use automatic renewal to ensure your critical domain names do not inadvertently expire
- Register and/or renew critical domain names for multiple year terms. In addition to security, longer registration terms benefit search engine ranking
- Establish an account password policy and regular password changes. Outline an escalation procedure and course of action in the event password leak occurs
- Create an e-mail account specifically for domain related communications. Choose a generic name, not that of an employee, and ensure this e-mail account is accessible only to your administrative contact and/or authorized personnel
- If your organization has authorized more than one administrative contact or employee access to your domain portfolio, make sure their names are on file with a designated security officer

For additional information please contact

Webnames.ca Corporate and Premier Services

Toll free : 1-866-470-6820

Email : corporate@webnames.ca