Domain Security Best Practices

With domain name security breaches on the rise, protecting your business-critical domains needs to be a priority. By following these domain security best practices, brands can reduce security vulnerabilities and protect their reputation, business continuity and revenue.

1. Lock Core Domains at the Registry Level, Wherever Possible

Registry locking should be applied to domains used for transactional sites, email systems, intranets and site-supporting applications. This elevated locking mechanism, which prevents erroneous name server updates, hijackings and social engineering attacks, freezes all domain configurations at the registry level until a customer-specified and registrar-specified, high-security protocol is followed.

2. Employ Two-Factor Authentication for Accessing Your Domain Management and DNS Management Portals

As an additional login feature, two-factor authentication helps protect your account against unauthorized access. By requiring users to enter a one-time security code in addition to their username and password, online accounts are protected in the event that login credentials are lost, stolen or compromised.

3. Never Share Login Credentials to Your Domain Management or DNS Management Portals

Sharing login credentials poses a security risk. Not only does it make it more difficult to identify the person making a change, it increases the chance of someone with malicious intent gaining account access and causing a serious security breach. Every account user should have a unique username and password.

4. Disable the Ability to Edit Core Domains for All Users

To further safeguard against unauthorized or unintentional domain modifications, advanced locking should be applied to your most valuable domains. By employing a registrar lock security feature, domains are made editable only when a high-security, pre-defined protocol is followed.

5. Continually Manage and Review Secondary Users

A frequent review of secondary account users is necessary to remove any users who may no longer be with the company or who may have changed job roles. It is also important to regularly review user permissions to ensure that proper permissions are applied to each user. Managing user accounts is critical in maintaining a clear list of current/authorized users of your account.

6. Require Mandatory Password Updates

Password management options can force password changes every 30, 60 or 90 days. Implement forced password changes to make it more difficult for scammers to gain access to valuable login credentials.

7. Implement IP Access Restrictions

Prevent unauthorized logins and protect against lost, stolen or compromised login credentials with IP access restrictions. This limits account access to specified IP addresses only.

8. Receive Automated Notifications of Every Domain Name Update

Secure account management allows automatic notifications to a specified, secure email address when any change to a domain occurs. Once enabled, this service will automatically send a system-generated email to the secure email address, notifying the recipient of any change that was made.

9. Utilize a Corporate-Only, Hardened Registrar

Ensure that your registrar employs a "hardened" portal—one that employs constant checks for security and code vulnerabilities. The registrar must have a proven track record of being able to stay on top of new exploits and of researching and understanding new vulnerabilities. In addition, the registrar must be able to demonstrate use of strong internal security controls and best practices.

For more information on developing a comprehensive online anti-piracy strategy, please call us at **1-800-745-9229** or visit **markmonitor.com**.