How to Protect Your Domain Name

Posted on February 15, 2017



Domain names represent the online identification of individuals, businesses, and organizations. Rising cyber security threats have time and again proven that individuals and organizations must protect their virtual assets against a range of threats or circumstances that may result in temporary or permanent loss of their domain name.

The threats a domain owner faces can be both external as well as internal. An external attack would be when a malicious entity tries to gain unauthorized access to a domain name registration account in order to control a domain name or to alter Domain Name System (DNS) information associated with that domain name. An internal threat can be in the form of a failure to renew a domain name, which can also result in the loss of your domain name.

Various measures are available for Registrants to protect their domain names against such compromises. Certain precautions that can be taken directly by Registrants are as follows:

Choose a suitable point of contact

When registering a domain, you have to list several contact people:

Registrant Contact
The Registrant is the legal owner of the domain. This should always be you, the business owner, not your web developer or anyone else.

Administrative Contact
This contact has the ability to change the domain record and represent the Registrant to the Registrar in administrative matters. Again, this
should be the business owner or someone who works in a position of authority and can be trusted.

Technical Contact
This person is in charge of dealing with any technical problems related to the domain such as DNS operation etc. It could be your system
administrator or an IT person on staff or you could also get your web hosting company to be apoint of contact here.

Billing Contact
This person is responsible for payment and other financial matters relating to the domain.

All these points of contact are very crucial as they have access to and can edit registration information of your domain. Ideally, all the four contact points should be different in order to protect your domain name, as in case if a single contact is provided for all the roles and that contact ceases to be employed by an organization it could get difficult for you. Also, if the only identified contact is not available to resolve a problem or respond to a reported abuse for the domain name, problems can arise. But do make sure that maybe except for Technical contact, all the other contacts are absolutely trustworthy and are placed within your organization. Do not ever allow an outside website designer or host to be listed as either the domain owner or administrative contact.

Protection against unauthorized account access

In the case of bigger companies who have multiple domain names registered, you should maintain a list of all the authorized contacts for each domain registration account. These authorized contacts should be made aware of their responsibility of protecting and safekeeping the account

credentials. Ideally, you should use different credentials for each account.

Place a registrar lock on your domain

Registrar Lock is a safety feature that prevents unauthorized domain transfers i.e the registrar for that domain has locked the domain to prevent any domain transfers, modification as well as deletion of that domain. This feature is very helpful in protecting your name against unauthorized transfers and hijacking.

Always opt for a registrar who offers this feature. Also, make sure that your registrar gives you the ability to automatically unlock your domain names at any time without going through any long and tedious process.

Importance of your key email account

Registrars send all communication with regards to your domain account to the email address provided during registration. Right from general notification to account modification to domain expiration/ renewal notice, your email is the primary way in which Registrar’s get in touch with you. Hence, this email account needs to be on a trusted platform and also be completely secured.

It is imperative that access to this account is given only to authorized and reliable people. If possible, avoid using a free e-mail address on your domain records. Also strengthening client authentication can help keep your email account secure. Use encryption (TLS extensions for SMTP) to protect mail client-server communications from eavesdropping.

Also, if you are using a spam blocking service, you run the risk of not receiving any notices from your Registrar if they are incorrectly categorized. You can prevent this from occurring by adding your Registrar to your ‘safe list’. This will ensure that all the communication from the Registrar makes it straight to your inbox.

Keep your contact information updated

Your domain name can be canceled if the information you have provided during registration is not accurate and you fail to respond to a Registrar's inquiries within fifteen days. Most reputed Registrars contact their customers on a yearly basis to verify their domain information and sometimes if your information has changed and you have not taken the time to update it, your

domains may be at risk of being deleted. Besides that as mentioned above, most notifications are shared via email by Registrar's so it is really important to check/ update your registration details periodically. This can also help you keep an eye on your domain account and make sure no malicious activity is happening on it.

Renew your domain name on time

Failure to renew your domain name can have grave consequences. A renewal lapse occurs when a Registrant does not renew his domain name and it expires, thereby allowing somebody else to register the same. Somebody may register the domain to sabotage the goodwill created by the brand or just to extort money from the earlier owner. Whatever may be the reason, it is best that you keep an eye on your expiration date so that you can avoid any such mishaps.

In case you know that you will need the domain name for many years, you should opt to renew your domain name for the maximum amount of time that your registrar provides. By doing so, you can avoid yearly registration hassles as well as prevent your domain from accidently expiring.

Maintain proper domain ownership documentation

Registrants should maintain proper documentation in the unfortunate event of any dispute or any other situations where there is a need to prove domain ownership. Certain documents that can come handy are:

- Copies of registration records.
- Billing records.
- Logs, archives, or financial transactions you have published.
- Correspondence to you from your registrars and ICANN.
- Any legal documents, tax filings, government-issued IDs, business tax notices, etc. that associate you, with the domain name.

Avoid brand infringement

It has become imperative for big organizations, as well as individuals, to ensure that your brand name or trademarks are not being violated or misused. Thousands of domains are registered or dropped every day, and it can be challenging to keep track of all of them. With Brand Alert API from WhoisXmlApi, you can accomplish this herculean task. You can easily monitor recently registered & deleted domain names everyday, across most gTLDs, which contain a trademarked word, product phrase, minor variations to your firm's brand or even a relevant keyword term. This can help protect your intellectual property and check potential trademark infringements through random searches to help reduce and eliminate domain name similarities, duplicates, or copycats. With Brand Alert API you get timely alerts so that you can take steps proactively to safeguard your brand.

Besides this, businesses can also opt for the Brand Protection Solution which provides a comprehensive Whois products and services data solution package that can help you to protect and build your brand.

As technology evolves, so do the tactics that cyber criminals rely on to identify and exploit potential vulnerabilities. The battle to protect your brand online is growing more complex with each passing day. The cost of inattention is potentially huge, leading to reputation damage, brand confusion and maybe even revenue loss. With the precautionary step shared above, Registrants, be it an individual or large companies, can try and increase the security of your domain name and also protect your brand!