The Definitive Guide To Never Losing Your Domain Name Again

We wrote this paper because we see it happen all too often....

Imagine at long last the moment arrives, it's finally time to kickoff that project you've had in your mind's eye for years. You knew it was inspired and game-changing from the moment you conceived it, and you even managed to register the *perfect domain name* for it, way back when you first thought of the idea.

The timing is right and the stars have aligned. Now it's time to assemble your team and start putting it all together, including the website. There's only one problem,

Somebody *else* now owns your domain!

Every year, millions of domains names expire. In too many cases it happens unintentionally, the owners miss the renewal notices for various reasons and they do not figure out that they are in the process of **losing** their prized domain *until it is too late*!

So many domain names are lost in this fashion that an entire industry has evolved around grabbing desirable domain names as their owners let them "drop" (expire). Great fortunes have been amassed on domains harvested via "the drop game". Once a domain goes "over the edge" in this manner, it's gone forever. The "domainers" move in: using sophisticated "name sniping" algorithms and dedicated "drop catching" software they grab an expiring domain name within milliseconds.

100% Percent of ALL Unintentional "Drops" Can Be Eliminated By Following These Simple Rules:

Rule #1: Always Register A Domain In Your Own Name or that of *Your* Organization

Domain names have registration records attached to them, they are called "whois records". (To lookup any domain's whois record, use a website lookup tool such as http://www.easywhois.com) Those records are broken up into sections:

The Organizational Contact
The Administrative Contact
The Technical Contact
The Billing Contact
Domain Creation, Modification & Expiry Dates
Nameserver Delegation
Domain Status

For purposes of this paper, we're most interested in the Organizational ("Org"), Administrative ("Admin") and Technical ("Tech") Contacts.

The important thing you need to know is this: Whoever or whatever entity is listed in the Organizational contact for a domain name for all intents and purposes *owns the domain.* We say "for all intents and purposes" because it is still nebulous in legal terms whether domain names are actual property, that can be owned, or simply convey rights to use. In fact it varies by jurisdiction, so suffice to say, whoever is listed here *controls the domain and holds all rights to it.*

Who is listed here? It should be **YOU.** Your name, your company or other applicable entity.

Too many times, what gets listed here instead if **YOU** are any of the following:

The personal name of an employee
An outside web designer, IT consultant or programmer
Your web hosting company
Your Internet Service Provider
Your Domain Registrar
An "anonymized" or "private" registration provider
Anybody else who isn't **YOU** or **YOUR COMPANY**

When this happens, you basically operate your entire web presence of your domain at the whim of whoever actually "owns" it: the person listed as the organizational contact.

The Admin contact is supposed to be a designated "administrator" for the domain. Many times these are *also* set as one of the entities above, sometimes for the ostensible reason that they are "administrating" the domain on your behalf.

In practice, even though the Organizational Contact "owns" the domain, all control over it is exerted via the Administrative contact. For this reason you should follow the same guidelines as for Organizational contact and make yourself or your company the Admin contact on all of your domains.

The only places in a domain record where it is acceptable and *harmless* to list third-party entities such as vendors or consultants are as the "Technical" and "Billing" contacts. These roles typically exert no control over the name and are used primarily as point-of-contacts between entities needing to communicate about various operational and network issues.

Action Steps:

Undertake an immediate inventory of your domain portfolio and make sure that you or your company is listed as the *both* the Organizational *and Administrative* contacts.

Draft a policy going forward for future domain registrations and who or what the Org and Admin contacts needs to be for future domain registrations. I.e Set the preferences in your Domain Registrar account so that future registrations automatically get created with this contact info.

Rule #2: Never use an email address in your domain registrations that is *outside* of your direct control.

We see this all the time: people use an email address at their ISP, some third-party mail provider like Hotmail, Gmail, their school, their work address, etc.

Understand that anything important that will ever happen with respect to your domain name will occur via email:

Domain Renewal notices
Transfer Requests
Authentication codes
Password resets from your Registrar
Notifications from Governing Bodies

When it comes to your own domain names, you want to make sure that those key emails are always being sent to an address that is itself inside a domain name that you control. Not your work, not your school, not your ISP, ***you***.

Even if you are just "redirecting" any email that comes to this address to your *real* email provider (work, school, ISP, Gmail, Hotmail, etc), at least **you** are controlling the flow of that email traffic.

ISPs go out of business. School accounts go stale and are closed down. You really never know what is going to happen to anybody else's domain name over the long haul. So make sure all key emails are coming to the one thing you *can* control: a domain name that you've registered using the guidelines in this report.

Action Steps:
Pick one domain name that will be your central point-of-contact email domain for your entire domain portfolio Register that domain for 10 years (the maximum possible term) or have it set to "auto-renew" with your Registrar Update the email addresses in all of your other domain names with an address inside this one domain.

Exceptions for easyDNS Members - What About MyPrivacy.ca?

Some users have rightly pointed out that our free service "MyPrivacy.ca" (See http://myprivacy.ca), which reduces spam you receive from your domain whois records may violate this rule. In a sense, it does. We feel confident continuing to recommend using myprivacy.ca addresses in your Whois records because *we* operate MyPrivacy and have no intention of ever terminating it.

Having said that, you should *only* use a myprivacy.ca address in your domain Whois record, you should *not* use it in your registrar member settings. Password resets and account access emails will be sent to your Registrar account email address, not your Whois address - and *that* email should very much be at a domain under your control.

Rule #3: Never Use "Whois Privacy", Privacy Masking or other "Domain Masking" services on a production business domain, be very careful on all others.

[Since we wrote this guide we have started offering Whois Privacy. You should read this section carefully before you make a decision on whether or not to use it. You can read about why we started offering it here: http://blog2.easydns.org/2012/05/16/the-official-easydns-flip-flop-on-whois-privacy]

The two big problems with Whois Privacy are that

#1) If you are not listed as the Domain Registrant in the domain's Whois Record, then you don't really own the domain, and

#2) When Registrars escrow their Whois Data with a third-party escrow service, it used to be the masked data which was escrowed.

In our case, we added a capability to our Whois Privacy option where you can still list your organization's name as the registrant of your domain, but anonymize everything else to cut down on spam.

Further, (at least here) we've arranged things so that your *underlying* whois record is escrowed on your behalf, instead of the masked record.

If you are going to use Whois Privacy with any Registrar, you need to double check with them which set of data is being escrowed.

When Should You Use Whois Privacy?

If you are registering a domain in a private capacity, a whistleblower or expressing dissent in some way, then you may need Whois Privacy and a sympathetic Registrar who will work with you instead of throwing you under a bus at the first sign of trouble.

Businesses Should Never Use Whois Privacy.

It is important to know that when consumers are dealing with an ecommerce website or online business, *private whois records are viewed with suspicion*. They often carry connotations of "hiding something", and with good reason: internet scammers typically use these services.

If you are operating an internet business that sells online, if you have "private whois" records (and in some cases you may not even be aware of it), it is quite possible that *you may be losing sales as a result.*

Action Step:

For Businesses:
Check if any of your domain names are using whois privacy and if so, disable it.

For Private Individuals, Whistleblowers, Etc.
Double check with your Registrar that your underlying data is being escrowed.

Rule #4: Consolidate Your Domains With One Registrar (and Choose That Registrar *Very Carefully)*

Most inadvertent domain drops are the result of poor organization, inconsistent methodologies or a total lack of methodology in managing one's portfolio. Domains end up spread around multiple Registrars, each of them using different contact info to communicate with you. Sooner or later one of those email addresses or point-of-contacts is going to slip off your radar, and then eventually your domains there will go with it.

The other fact you need to be aware of is this: Because expiring domains are so lucrative, many Domain Registrars *actively* mine the pipeline of *their own customers' expiring domains*. They do this by monitoring the traffic to them during the expiry cycle and when the "good ones" are ready to go over the edge, they **renew those domains at their own expense** and **then keep them**, transfer them to a related party, or sell them off.

Since you, the Registrant's rights to the domain did expire when the domain did, this is permissible conduct under the Registrar accreditation rules. Some Domain Registrars make more money doing this than they do operating in the normal course of business.

So it helps to have all your domains in one basket. If possible, try to develop a relationship with that Registrar. This is hard to do with some large companies where you will never talk to the same employee twice, and may be an argument for going with a smaller, more personalized company who can get to know you and you them.

People may be afraid to go with the smaller Registrar because they wonder about its viability going forward for the long term. They figure the big company may be impersonal, but they're "too big to fail", so their domains are "safe" with them.

What you should know is that the governing bodies who oversee all Registrars have in-place procedures to provide continuity of service in the event of any Registrar failure. Further, all Registrars are required to backup their customer domain data into a third-party data escrow service.

In the event of a Registrar failure (large or small, for whatever reason), that Registrar's customer domains will be transitioned to a new Registrar using the data in escrow.

So don't fall for the "bigger is better" argument for Domain Registrars. There are numerous anecdotal cases (just search google on "Domain Registrar nightmares" or something similar, where a large bureaucratic Registrar "took down" a domain on the flimsiest pretext without putting any critical thought into what they

were doing.

A good way to source out a Registrar is via a fairly simple 2-step checklist:

> Send them an email. See if you get a form response, a personalized response with some thought behind it, or any response at all.
> Call them on the phone. How long did you hang on hold? Was it voice-mail hell? How did they treat you when you finally got somebody on the phone.

The whole point of a Domain Registrar is that you can rely on them to interact with you promptly, courteously and professionally *that one time when everything hinges on it* (i.e. when you're about to go on CNN to talk up your project and you realize the website domain is down).

Action Steps:
Put Your Registrars Through the 2-Step Test, then Select a Single Registrar and Consolidate Your Domains There Send them an email. Gauge the Response in terms of response time, reading comprehension, genuine (not canned) responses and helpfulness. Call them on the phone. Measure wait times, complexity of voicemail menu, demeanor and professionalism of your call agent. Are they trying to help you or upsell you?

Rule #5: *Never, Ever,* Intentionally Let a Domain Expire with the Intention of Re-Registering it Elsewhere.

We've had to warn clients away from doing this countless times. They have a domain name "stuck" somewhere for one reason or another. Bad contact info, defunct email address, non-responsive registrar, etc.

Sometimes people are tempted to simply "let it drop" because they think they'll just be able to re-register the domain the next day.

For starters, it doesn't work like that. Once a domain name expires it goes into an expiry process that takes from 70 to 80 days to play out before the domain finally "drops". And when it does, then if the domain has any marginal value whatsoever, it will be snagged by the drop catchers within milliseconds.

Whatever your situation is with the domain name you want to secure, take the hard road and work on a way to recover your domain. Having a helpful Registrar who can "go to bat" for you can work wonders in cases like this.

The following rules are geared more toward unauthorized domain transfers away from your account, as opposed to inadvertent "drops".

Most of the "unauthorized transfer" attempts we've seen over the years actually originate with an "inside man" or somebody who was formerly on the inside of an organization: a disgruntled employee, a former employee who has been fired, or an outside consultant with a billing dispute *(recall Rule #1*).

Rule #6: Always Enable the "Domain Lock" for Your Domains

Domains registered under most common top-level-domains like .com, .net, .org, .biz, .info run on a registry protocol called "EPP". Under that protocol domains can be "locked", also known as "transfer lock". When this lock is engaged, all attempts to transfer your domain name will fail.

While the vast majority of all inadvertent domain losses are the result of accidental domain expiry, there are occasional attempts to "hi-jack" a domain name. This basically means that it is not unheard of for a third-party to attempt an authorized transfer of your domain.

A slightly less sinister, albeit more pernicious variation of this is known as "domain slamming". That's when unscrupulous companies send you what *look like* legitimate domain renewal invoices, but they are really cleverly disguised attempts to get you to transfer your domain to a new registrar!

When this happens, you still retain ownership of your domain, but it is possible for the web services built atop of that domain (like your website, your email server, etc) to stop working as the domain switches over to the new provider. See http://www.domainslammers.com for more information about this tactic.

A general rule of thumb: Domain Slammers often send *postal mail* to try to get you to switch your domain over to them. Your actual Domain Registrar will more likely send your *real* domain renewal notices via email.

It is also a requirement of all accredited Registrars that they either provide you with real-time access to your lock, via a web interface, or that they follow your directions to lock or unlock the domain. We recommend using a Registrar that pushes control over that lock directly back to you in your web interface account.

Action Step:
Check the "Lock" On All Your Domains and Make Sure They Are Enabled.

You can use a whois lookup tool like http://www.easywhois.com to check the lock status of all your domains. What you want to see is something like this when you look at the whois record:

Domain status: clientTransferProhibited
Domain status: clientUpdateProhibited

If you see this:

Domain status: ok

It means the domain is **not locked** and you should immediately set that domain lock.

Rule #7: Enable "Login Notifications" for your Registrar Account

Whether it's a disgruntled employee trying to walk out the door with a domain name, an outside consultant with a billing dispute, or a legitimate session from somebody telecommuting from home, it is always helpful to know when somebody is accessing your account holding your domains with your Registrar and from what IP address those logins are originating.

This can be accomplished by turning on "login notifications", if your Registrar supports them. It is advisable to have these notifications go to an email address that will be seen by yourself and/or your lead systems people or whoever manage the domains for organization.

It won't take long for people receiving these notifications to get a feel for the normal usage patterns, so when a login occurs that deviates outside those usage patterns, the relevant people within your organization will know it sooner rather than later.

Rule #8: Protect your Registrar User Account with Additional Security Measures

Some Registrars allow you to limit logins to your account by IP address, hostnames & hostmasks and even country of origin. This can save your domains in situations where your account login credentials have somehow been compromised (see Rule #9 below).

For example, if you set your account so that it can only be accessed from within your company's local-area-network behind a firewall, then even people who know your password would not be able to access the account unless they were physically within your company premises or logged in via a VPN.

While no substitute for strong passwords and a rigorous security policy, this cuts down what are known as "attack vectors" significantly.

Rule #9: Be Aware of "Phishing" and "Domain Slamming" Attacks

We mentioned "Domain Slamming: earlier in Rule #6. This is when unscrupulous registrars send you deceptive looking "Renewal Notices" which don't actually renew your domain but instead transfer management of them to a new Registrar.

The easiest way to mitigate against this is to educate your accounts payable department about your vendors. Show them what a real renewal invoice looks like and direct them to discard or seek additional approval

internally for any domain related request that does not conform to your accepted, in-place renewal notices with your existing Registrar.

A more sinister variant of "domain slamming" are "email phishing" attacks. You may already be familiar with these when you get fake "online banking" notices that are trying to entice you to a fake website, posing as your bank where you try to log in and they steal your login credentials.

The same thing happens with domain Registrars, where domain hackers try to harvest login details for user accounts at a real Registrar by sending fake notices to you pretending to be from your Registrar.

You can guard against this by making it a point *never* to click on a link sent to you in email that is purporting to send you to your Registrar website, unless you are absolutely sure (by checking your browser's "location" bar) that you are actually on your Registrar's website when you get there.

Further, you should always login to your Registrar account using "SSL", a type of encryption used for securing web sessions.

You know you are connecting via SSL when the link starts with **https://** as opposed to just **http://**.

A better tactic is once you are securely logged into your Registrar's website: **bookmark** that website in your browser, and then always use that bookmark for future logins to your Registrars' website. So when you receive an email that asks you to perform an action, instead of following a link in that email, use your local, tested and validated bookmark to get there.

Conclusion:

The vast majority of unintentional domain losses are a result of disorganization, stale contact info and some kind of "lock-out" situation. By following these simple rules, you will always have access to your domain names and be receiving those important domain renewal notifications from your Domain Registrar.

In the minority of cases where domains are transferred to unauthorized third-parties, these are usually pseudo-inside-jobs: where the party grabbing your name is a former employee or a consultant who at one point had legitimate access or a mandate to control your domain but has since run afoul of the company.

For rare cases of hijack attempts by unrelated third-parties, or more common "domain slamming" attempts, education is the key to guarding against them. Make sure everybody within your organization who is responsible for managing your domain names reads and understands this report.

Below are a few "bonus tips" to further bullet-proof your domain portfolio:

Bonus Measures:

> Have the email address that receives your renewal notices "explode" out to multiple people within your organization. This is done by setting that address as a "mail alias" that forwards to multiple addresses. Some registrars provide "email forwarding" services bundled with your domain name and provide the capability to do this within your control panel where you manage your domain names.

Whitelist your Domain Registrar's email address. Add the "From" address in the email notices you receive from your Domain Registrar to your mail client's "white list" so that your renewal notices are not filtered out of your sight.

If your Domain Registrar provides alternate notification methods of domain expiries and renewals, turn them on. For example, easyDNS enables an iCal feed of your domain expiration dates which you can subscribe to using iCal (on a Mac), Google Calendar or any other calendaring client that supports the iCal protocol. (Not to sound biased, but we mentioned ourselves by name here because we're the only Registrar we know of that offers this.)

Copyright & Credits:

You may also be interested in:
10 Things You Must Know Before You Register A Domain Name With Anyone
http://web.easydns.com/10_things_to_know_before_you_register.php