SWCP Portal
November 2016

Who gets the gold, and who gets goosed?

Domain Transfers Just Got A Lot More Complicated

Important developments are happening behind the scenes regarding who runs the internet. Some involve **ICANN**, the **global internet name and address authority**, which has ordered major changes in the process of updating internet domain name registrar records.

These particular procedures have been in the works for long time. They will affect *all* changes in domain ownership from now on. Yet if the process is handled improperly, it could trigger a lock down on *any* domain status changes for at least *60 days* and cost owners more, too.

SWCP has been working with our longtime registrar, **Tucows/OpenSRS**, to make the new system as easy and effortless as possible. The changes are such, however, that some explanation is necessary, yet the more one reads the more confusing the whole thing becomes. Just like taxes.

Domains for almost everything

Remember when most domains ended in **.com**, **.net**, **.gov**, **.mil**, or **.org**? Those endings, called **top-level domains**, indicate the basic category the website fits into, .com meaning "commercial", .org "nonprofit organization" and so on. **Country codes**, to designate geographic locations, like **.us**, were meant for everything else.

The desire for short, memorable names, however, soon led to squabbles over ownership, costly scalping and speculation, the use of nonsense syllables, as well as names deceptively similar to better-known brands to lure people in.

The good news is that all of that is largely no longer necessary. Over the last several years, the entire domain system has exploded into over a *thousand* **top-level domains** now available. From **.abogado** to **.zoned**, users can get their sites into almost any category imaginable.

The bad news is that each one of these has different terms, conditions, and prices. For instance, anybody wanting a **.law** domain must provide documentation of being a qualified lawyer. Others are limited by particular companies – **.apple** usage is **controlled** by Apple, Inc. for example – or are limited to specific regions, like **.asia**.

And some are just plain pricey: a **.luxury** domain costs a cool *$550* for one year's registration. However, small discounts apply for longer terms, so if one registered it for 2-5 years, it would be *$540*/year and for 6-9, a mere *$525*. Similar discounts apply across the board. Our **Domain Pricing** page has a handy searchable table listing all *656* top-level domains that SWCP can service.

Rules for almost every situation

Such a system is complicated enough to begin with. Where it gets crazy now is in trying to transfer the registration of the domain name.

Changing the organization that officially manages the registration – the **registrar** – often happens when it's time to renew. SWCP prefers **Tucows/OpenSRS** to Go Daddy or Network Solutions for a number of reasons, so we encourage customers to use them also.

However, the transfer period historically provides the easiest opportunities for unscrupulous **domain hijacking**. Therefore, ICANN, in its wisdom, decided to make the entire process more secure by designing it by committee to be very complicated. What could possibly go wrong?

A lot, actually. Here's how it supposedly works:

1. *Any changes* to the first or last name of the owner, the organization, or email address fields for any domain name will now start a complicated confirmation process.
2. This involves obtaining *explicit confirmation* from current and new registrants before *any* changes can be completed.
3. After a change of registrant has been finalized, the previous and new registrant have to

receive notifications with *no option* of reversing the change.

4. Once this has been done, the domain is then *locked by default* for transfers to a new registrar for the following *60 days* just to be sure.

But if this is not done *exactly* right, the process triggers a lockdown while another slew of confirmatory emails goes around. The process has become so complicated that ***six different scenarios*** with different steps have been devised to try to protect domain owners from hijacking throughout the process.

For a site owner retiring and designating a successor or even simply changing their email address, this could become a real nightmare as *any* mistake could have expensive repercussions that linger for years. So Southwest Cyberport is doing all it can with Tucows/OpenSRS to make sure the process meets all of ICANN's byzantine rules and is as simple and foolproof as possible.

The solution is to name Tucows/OpenSRS as the **Designated Agent** through SWCP. This allows them to make changes in the user's name rather than depend on volleys of emails. Therefore users *must* sign the **Domain Registration Agreement** before registering new domains or transferring or changing any old domains.

Doing so will avoid the automatic 60 day lockdown and make it much easier for all concerned. Therefore **SWCP will be sending out emails to all domain owners requiring them to sign the *Domain Registration Agreement* before December 1, 2016.**

Note that this process *only* relates to domains registered through Tucows/OpenSRS. At this point, we do not know what other registrars have planned. Actual domain transfers will have to be handled very carefully to avoid lockdowns.

And domain owners will still have be wary of **spam** from shady registrars whenever their domains come up for renewal. Check with SWCP Tech Support with any questions you have.

One last note: **Whois privacy** that keeps domain owner contact information private is no longer free. We now have to pay for the WHOIS Privacy service, which we are passing on at *$5*/year/domain. Sadly, the domain name system increasingly resembles the golden goose of fable, but we're not the ones trying to hoard all the eggs.

Don't Become Part of the Botnet of Things

Several massive internet outages in the news recently **appear** to be aimed at learning how to take down the net. These have been **denial of service attacks**, where a site's servers are overloaded by a massive flood of requests coming from a vast, dispersed army of infected devices organized into a robot network or **botnet**.

What makes these attacks different is that the infected internet-connected devices are *not* PCs or servers, but are unsecured webcams, baby monitors, thermostats, lights and so on. **Over 100,000** were involved in the latest attack.

Though the sites targeted were American, few attacking bots were in the US. Most were cheap Chinese Internet of Things devices in China, Vietnam, Indonesia, Brazil and Spain. They had been hacked with **Mirai**, open-source malware specifically designed to build botnets by identifying vulnerable appliances over the internet.

Since the virus constantly scans the net, rebooted devices can be reinfected in as little as *10 minutes*. Even more troubling is that the malware is **open-source**, and enhancements have already been seen in the wild. There will doubtless be more tweaks, and the virus could be adapted for other kinds of attacks – including **ransomware**.

With the holidays fast approaching, and internet-enabled toys and gizmos being all the rage these days, it behooves consumers to be *very* careful. Security costs extra so do not buy the cheapest devices. In fact, it's safest not to hook up *any* internet-connected device unless it is at least **password-protected** *and* the user can change that password. Then be sure that you do, or mention it in your gift note. It's not much, but it may help everyone to have happy holidays.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) ◉ **SWCP.com** ◉ **Help@swcp.com**

5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.