.si News

.SI TLD NEWSLETTER

register.si

No. 1/2013

publisher: ARNES • **editor:** Milijan Plužarev • **design:** KOFEIN • **Ljubljana, August 2013**

Domain name hijacking

Is your domain name safe? If you are not prepared, there are a number of common mistakes which can result in the permanent loss of your domain name. While many people think that domain name hijacking is carried out by hackers and e-savvy business competitors, perpetrators are often ex-business partners, angry clients or ex-spouses trying to get back at one another.

Domain name hijacking is when someone changes registration data of a domain name without the original holder's permission. Usually this happens by someone pretending to be the domain name holder and convincing the registrar to modify the registration information. Once this information is altered, the hijacker can then transfer the domain to another registrar and take control of websites and emails.

TOP 5 TO KEEP IN MIND

→ **Always maintain accurate contact information with your registrar or services provider.**
In the event of a theft it will be difficult for a registrar or service provider to determine who the rightful registrant of a domain name should be.

→ **Register your domain names with a reputable registrar.**
There are many registrars to choose from and hundreds of resellers.

→ **Never allow your listed emails to expire.**
Your email address is the key to unlocking your domain names.

→ **Keep usernames and passwords secure.**
Do not share these with anyone, unless there is an absolute need to.

→ **Monitor your portfolio.**
Routinely monitor your portfolio for any unauthorized changes.

COMMON FORMS OF DOMAIN HIJACKING:

- Impersonation of a registrant in communications with a registrar.
- Registering a lapsed registrant email address to reset password and authorize a transfer.
- Registering a lapsed domain name used for registrant email address, and then spoofing the email address.
- Hacking or spyware.
- Forgery of transfer authorizations or other account verification information.
- Theft by a disgruntled company employee or business partner.
- Hijacking an email server to spoof email to make it look like it came from the registrant.

PLAYING IT SAFE:

- **Be careful who is listed in your contact information.** Make sure that all the contact information listed with your registrar is accurate and up-to-date.
- **Keep track of your domain names' expiration dates.** One of the easiest ways to lose a domain name is by forgetting to renew it.
- **Be careful when replying to official looking notices you receive by email.** It is better to contact your registrar directly and make sure this correspondece is genuine.
- **Be careful when using free e-mail addresses.** Many free email services will automatically suspend or delete your e-mail account if you do not log in frequently enough. A hijacker can sign up for your same email address.
- **Add your registrar's and registry's domain name to spam filter's approved sender list.** Important notices are of no use if they are in the trash or spam folder.

WHO'S WHO

REGISTRANT
- Domain name holder.

REGISTRAR
- Company authorized to register domain names.

REGISTRY
- Organization that keeps the database of a top-level domain name.

IMPORTANT LINKS

http://registry.si
- The registry of .si top level domain name.

http://varninainternetu.si
- Slovenian webpage about safety on the internet.

http://cert.si
- Slovenian Computer Emergency Response Team.