Domains & DNS

I received a domain expiration notice that isn't from BRI, is it a scam?

First and foremost, if your domain is registered with Brownrice, your expiration notices will always come from a Brownrice email address. If your site is hosted with us, but your domain name is registered with another company, Brownrice will still send you expiration notifications as a courtesy, although we cannot renew 3rd party domains for you. You may also receive such notifications from your registrar.

The email you receive from Brownrice will state clearly that you can either click a link to renew with us, or it will advise you to contact your registrar. We do our best to alert you to any expirations, but we can't keep track of all your domains if they aren't registered with us. When in doubt, email support@brownrice.com and we'll investigate for you! But always keep in mind:

You can EASILY avoid most scams yourself!

Do they want an exorbitant amount of money for the "renewal", say $50-$60 or more? Some "premium" domains may cost that much, but the average .com, .org, or .net should never be that high. If you are being charged that much, you may need a new registrar.

Look at the FROM address in the email you received. Is it from a reputable company you may have done business with, such as GoDaddy, Enom, Tucows, etc?

Great! Still skeptical? Forward it to support@brownrice.com, and we'll tell you if it's legit!

Or...

Is it from a Gmail, Hotmail, AOL, or other "freemail" address? Is it from a party you've never heard of, or a seemingly random address, like ing97[dot]org, or superawesomeSEOservices?

If so, Delete it, and go on with your day.

Look for keywords!

Such as "solicitation", "SEO" , "proposal", "offer" etc. Look for UNSUBSCRIBE links at the bottom. Your registrar will rarely, if ever, offer an option to opt out of expiration notifications, as doing so could result in you losing your domain name. If you find any of those items, chances are it is a scam. Do NOT click on any links in that email. Either delete the email, or add it to your junk / spam filter.

Was it written by an infant?

Look for lack of punctuation, nonexistent grammar, broken English, ALL CAPITAL LETTERS, and truncated text that looks like it was copied and pasted, or written by a computer. This should go without saying, but we'll say it anyway: these emails are bad. Beware of incoherent emails asking for money. Just because they know your name and your domain name, does not make it legitimate.

Be smart, be safe, never enter your payment info when in doubt. If you have questions, just ask!

Unique solution ID: #1290
Author: n/a
Last update: 2018-02-13 07:54