

Fifth Largest Internet Domain Provider Gets Hacked but Much of Data Was Encrypted

October 31, 2019 - Web.com, which also owns Register.com and Network Solutions has confirmed that all three of its domain registration services were hacked sometime in August. The company is responsible for managing the registration information on more than seven million domains. While the hack may prove to be a windfall for spammers, it appears that it is unlikely to lead to identity theft; largely because the company did what it should. They encrypted critical data.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

Anyone who has ever registered a domain has had to hand over a lot of personal information. That includes names, addresses, email and credit card information. The process also requires you to come up with a password to manage your new domain.

Much of the data provided is stored in the open unless you pay additional fees to keep your information private. There are services, such as WhoIs that can be used to look up the owners of domains. Typically, you can look up the name and other contact details for the domains owner. That information is there for anyone to see.

But what about the credit card and password data. Can that be seen too? Well, apparently Web.com actually used encryption the right way... which is more than we can say for a lot of companies. While they did store this type of data, they also encrypted it. In the company's announcement on the breach, this fact allowed them to state that they think the data is safe and that their clients don't have to worry about fraud. They also believe the same to be true for passwords.

They are advising customers to keep an eye on their credit card bills and to change their passwords as a precaution. But keeping an eye on credit card bills is always wise and since people often reuse passwords on multiple sites, changing passwords after any data breach is advisable... whether or not the data is encrypted.

Unfortunately, the one thing that the company's customers should expect is an uptick in SPAM. If you can change the email address associated with your domain name, that would probably also be wise since this contact information is normally stored in the open.

No data breach is good news, but it is nice to know when a company that stores a lot of consumer and business data is doing something to protect it. It's an example that everyone else should look at closely.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS