The value of . iwi.nz

Author: Karaitiana Taiuru

.iwi.nz Moderator 2000-Present

Date: March 2012

The same issues corporates and businesses face in the online world in regards to branding and identity are also faced by Iwi. There is no difference between the commercial and Iwi groups and many other Indigenous Peoples of the world. The only exception is that Iwi have an authentic and protected area on the web with .iwi.nz .

.iwi.nz is a specifically Iwi/Hapu/Taurahere Ropu only web address that is moderated by a real human who checks the authenticity of Iwi names and declines names that are not being registered by the Iwi. Only one company has the authority to register .iwi.nz names which further offers authenticity and security in .iwi.nz and is a further assurance to web site visitors and whānau that the web site they are visiting is really the genuine Iwi web site.

The importance for Iwi to register only in .iwi.nz is vital to ensure that Iwi protect both their online identity and for the online safety of Iwi members and whānau.

The issues of a non .iwi.nz address.

So often we hear of a web search for a tribe that takes a user to a gambling web site, an imitation site offering fake jewellery and resources or to pornographic content.

In New Zealand the issues for Iwi have faced is people who register Iwi names out of the .iwi.nz address and then offer them for sale at sometimes hundreds of dollars the price to register the name in the first place.

Another issue that Iwi face is having thier genuine web site duplicated so as it looks the same as the genuine Iwi web site. The scammers then use the fake site to gain personal information, credit card details etc. If this occurs, you will need to make a complaint to the Domain Name Commissioner Dispute Resolution Service.

Or a site is registered with the Iwi name out side if .iwi.nz and appears first in Google searches. This issue can be combated by asking your web developer or expert to make your web site rank higher in search engine rankings by using key words etc.

Previous widespread issues.

When .maori.nz was launched in 2002, a businessman bulk registered the majority of Iwi names and then offered them for sale. Likewise in 2012 the launch of the new .kwi.nz domain name saw a handful of individuals register Iwi names. In 2013 The New Zealand Maori Internet Society began its investigation and logged formal complaints about several of the names.

Potential issues on non .iwi.nz

Imagine someone searching the Internet for an Iwi organisation and finds IWIname.maori.nz and registers their personal details in a manner one would expect to find on an authentic Iwi web site. But unbeknown to the visitor, the web site is run by criminals who now have a database of contact details of whānau and individuals. It is very simple to do and is often seen with criminals registering names similar to a bank or other business name and creating almost identical web sites. It is called a phishing attack and happens more often than most people think.

Another common trick that online scammers use is ascertaining commonly misspelt word variants and registering those as genuine web addresses. For Iwi there is the added security concern that macrons can be added into web addresses, hence ngāi or ngāti can be added to a web address. Again this is another reason to use .iwi.nz as it is almost impossible for any fraudulent names to be registered, or at least for very long without the contact details of the person being recorded and the address cancelled.

If you do find yourself the victim of cybersquatting there are options available.

1. The legal manner is to visit the Domain Name Commissioners (DNC) web site and use their Dispute Process http://www.dnc.org.nz
2. A social (and legal) manner that is often equally effective is to look at the registration details of the person/organisation who has registered the domain name by visiting www.dnz.org.nz and searching from the box on the left hand side. If the details appear to be false, such as a registration name being Mickey Mouse etc, you can complain to the DNC about false whois information.
3. If the information is legit, it is public information and in the past has been published online to show the cybersquatters for what they are. This typically leads to a quick resolution.