Marine Corps Data Breach May Imperil Lives of Marine Reservists And Could Lead to ID Theft

March 1, 2018 - A data breach at the US Marine Corps Forces Reserve has released highly sensitive data on members of the US Marine Corps Reserve and their families. A mail messages was sent to the wrong email address with an attachment containing the personally identifiable information on more than 21,000 Marines and civilians. The message and the attachment were unencrypted and included names, SSNs, home addresses, bank accounts and routing numbers and emergency contact information. The breach raises a number of troubling questions; not the least of which is why was this data stored or able to be transmitted without encryption?

This breach is more than an inconvenience for those whose information was leaked. It may actually place them and their families in danger. A few years ago, ISIS prepared a kill-list naming active duty US military personnel. The list was assembled from social media accounts used by American military personnel to communicate with their friends and family.

In this case, the data being transmitted was intended to be used by the Defense Travel System to assist Marines, their families and civilian contractors when scheduling travel. Once the Marine Corps realized the mistake, they attempted to recall the message; something that was possible for other recipients that were on the usmc.mil domain. Unfortunately, some recipients of the message were outside of the military domain. Even if those who erroneously received the email properly destroyed the data, it is possible that any message transmitted in the open on the internet could have been intercepted.

The data included in the message attachment was apparently enough for cyber-criminals to commit identity theft. It also provides a roadmap straight to the front doors of everyone whose information was contained in the attachment.

The Marine Corps is in the process of notifying those affected by the breach. Anyone receiving notification should consider changing their bank and credit card account numbers and placing a security freeze on their credit files. Additionally, victims may want to carefully consider their home security needs. While there is no indication at this time that the message was intercepted by anyone, once information is out on the internet, it is usually out there forever.
byJim 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 me on Twitter:

Follow ACCESS