

# The Virgin Islands Consortium

## In Latest Phone Scam, VI Residents Are Hacked, Lose Money And Private Info Compromised

VIC News / **Published On December 09, 2015 10:10 AM /**

Staff **December 09, 2015**



ST. CROIX -- The latest telephone scam affecting the territory appears to be the most effective and dangerous, according to a press release the Department of Licensing and Consumer Affairs issued on Tuesday.

According to the release, residents are receiving phone calls from callers with foreign area codes such as Belarus, China, Afghanistan, Serbia and Latvia among other places. The reported area codes are 371, 375, and 381, and the name of the country associated with the area code generally appears with the number. The numbers are longer than the 10 digit numbers that emanate from a call made from the western hemisphere. Calls may appear from area codes other than those just indicated.

When such a call is received, the caller may ring once and hang up. The curious receiver of the call may then call the number back and as a result is charged \$15 to \$30 for returning the call. Or, the receiver of the call may answer the phone thinking it is a legitimate call. In both instances, the release says, the time spent on the call allows the possibility of the foreign caller to remotely hack any private, personal and sensitive information one may have stored on their phone, including contact lists, bank account information and/or credit card details.

In furtherance of the scheme, once contact information from one's cell phone has been stolen, the caller may make contact again, this time posing as one's cable provider, internet service provider, bank or other business establishment based on information only gotten through the original hacking of the phone. The foreign caller then attempts to swindle individuals through some other type of ruse.

Even if not successful in their secondary swindle, the hacking of personal, sensitive and confidential information is the scammer's aim, according to the release. Obtaining such information is, in and of itself, of value to the scammer and may work to the detriment of the owner of the information.

In light of this latest fraudulent scheme, DLCA is advising consumers not answer phone calls from foreign jurisdictions or from other places that one knows he or she has no business or personal contact with. If and when messages are left from these calls, be circumspect and cautious of the fact that no matter how authentic the message may sound, calling the number back may result in the compromising of personal, private and sensitive information stored on one's cellular device.