

Article from **Dealer Magazine** ([http://www.imakenews.com/dealercomm1/e\\_article001629832.cfm?x=b11,0,w](http://www.imakenews.com/dealercomm1/e_article001629832.cfm?x=b11,0,w))

December 22, 2009

## **Web site identity theft**

*by Gil Van Over*

The Federales have a multi-pronged, largely unsuccessful approach to stemming the tide of identity theft.

Why just last week, one of my associates received a phishing e-mail that looked like it was from a national credit card company. The same day, coincidentally, my wife received a replacement credit card by overnight express from the same company because her card had been compromised.

While we have been inundated with all of the stats and hyperbole about our individual identities at risk, not many of us who have websites think that our Web site will be compromised. Think again!

A dealer recently found out that someone posted a phone web site that looked suspiciously like his.

This phony Web site had the dealer's name and address, listed an inventory of over 100 low-mileage cars, contained links to fake anti-fraud Web sites and provided phony certifications. Problem is that whoever put the Web site together advertised prices at about a third of what the vehicles should sell for.

Of course, the dealership was deluged with calls and orders.

Of course, the police apparently have other cases to work on.

Of course, the scammers have hidden behind a layer of cyber clouds.

I guess it makes sense to periodically conduct an online search using your company's name to see what is out there.

*© 2009 by gvo3 Consulting, LLC. All rights reserved.*

Published by [Dealer Communications](#)

Copyright © 2010 Horizon Communications Inc.. All rights reserved.

Information in this newsletter is provided by both proprietary and public sources. Dealer Communications makes no claims as to the accuracy of information provided by third party providers.

Powered by [IMN](#)