**SECURITY Identity, Email, Cell**

Over a billion dollars is lost by unsuspecting innocent consumers each year to scams. The bad guys are getting more sophisticated and trying to breach our privacy and financial security via email and phone.

* ***Never give your account information or SS# over the phone*** to someone calling stating that they represent your bank or credit card; ask them for a number to call back and compare that with the legitimate numbers on your credit cards and statement(s)

[This Photo](http://womentakingastand.blogspot.com/2011/11/answering-call.html) by Unknown Author is licensed under [CC BY](https://creativecommons.org/licenses/by/3.0/)

* ***Never send your personal info over email*** in response to “PHISHING” scams where the email states that your bank account or credit card has been breached and they need your info to properly identify you

[This Photo](https://lengualia.wordpress.com/tag/ortografia/) by Unknown Author is licensed under [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)

* ***Never answer your cell phone if you do not recognize the number***. “VISHING” is when the criminal uses a VOIP automatic dialer to randomly call cell phones. The number and location that appear on your cell phone are random, thinking you’ll be intrigued enough to answer a call from another city across the U.S. Once you answer and go through the menu or even press zero to speak to an operator, your phone and information on it could be copied or “spoofed”

[This Photo](http://groundreport.com/well-heres-another-fine-mess-youve-gotten-into-what-a-difference-a-l-makes/) by Unknown Author is licensed under [CC BY-NC](https://creativecommons.org/licenses/by-nc/3.0/)