

# Phishing ... For Your Bank Account



Richard W. Schierer  
December 2009

Between my business and personal email accounts I get about 200-250 emails a day. Some are e-newsletters, association notifications, networking events, forwards from friends, etc.; you name it I get it! Most end up getting deleted without even a thought.

The ones that catch my eye are the ones from known business associates, vendors, family and friends and from 'my banks'. 'My banks' don't send me emails. And if you ask your banks, they will tell you that they don't normally send emails to their customers.

Most emails from banks are 'Phishing Schemes'. "Phishing is the [criminally fraudulent](#) process of attempting to acquire sensitive information such as usernames, [passwords](#) and credit card details by masquerading as a trustworthy entity in an electronic communication." (definition from Wikipedia) They state that it seems that their database has become corrupt and they need me to click on the enclosed link that will take me to their website where they want me to enter my username and PIN.

PC security rule of thumb says NEVER follow the link in an email from anyone you don't know. (and always think twice about clicking on one from a friend.) The problem is that the email is not from my bank. The email is from someone trying to get my username and PIN so that they can empty my bank account!

If you look at the email address that the email came from, it almost looks like it might have come from your bank. But there are usually

extra words or letters. For example, my bank is the Bank of America. Their emails come from [info@bankofamerica.com](mailto:info@bankofamerica.com). Someone trying to phish my account information might use [info@bankamerican.com](mailto:info@bankamerican.com). And the link that is included in the body of the email might say Bank of America, but if you roll your mouse over the link it will show you the true internet address in the bottom left-hand corner of the email. The link can say anything it wants, but the true address is where you would be re-directed.

And upon arrival to this bogus website you would get fooled again because chances are they re-created your banks website down to the last picture. Again you would think you were ok, but as soon as you entered your username and PIN (count to ten now) all your money would be GONE! It would be that fast!

I have gotten these emails and have called my bank. They have acknowledged that the emails are bogus and ask that I forward them to a specific email address where the bank can try to track them down. The chances of this are very low. Most scams take place from overseas and they send out hundreds of thousands of emails. And sadly even if they only get 1/10<sup>th</sup> of 1 percent of them, they are doing good.

So please, (as Elmer Fudd used to say) "Be very very careful" when opening emails from anyone. Even emails from your friends and family can be compromised!



Richard W. Schierer  
[makemytechnologysimple.com](http://makemytechnologysimple.com)  
631-375-4512