

# Financial "Phishing"

Have you received an email like the one below?:

Dear Regions Cardholder,

Continuous Monitoring is an integral part of Regions Bank multiple layers of security. In addition to other fraud monitoring tools, we can often spot fraud based upon transactions on the card that are outside of cardholders typical purchasing pattern. This allows us to spot fraudulent activity as quickly as possible and acts as an early-warning system to identify fraudulent activity.

During a recent checkout we detected suspicious activity and your credit card may have been compromised. Fraudulent activity made it necessary to limit your card for online services, your case ID number for this matter: AT09GP32D506 : Conform to our security requirements and in order to continue online services with your card, we must validate your identity.

Please use our link below to proceed.

<http://0xdc.0x82.0x32.0x65/.secure.regionsnet.com/EB/logon/VerifiedByVisa/index.htm>

Regions Bank takes online security very seriously so that you can shop safely on the Internet. As part of our commitment to fighting fraud we have the right to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of the terms and conditions.

© Copyright 2007, Regions Bank - Financial Corp. All Rights Reserved.

This is called "phishing." It looks very real, very official with a copyright at the bottom and the link to follow to take care of your "critical issue." However, the actual people sending these emails are trying to get you to click on that link, which does not go to your financial institution, and travel to a site they have set up to resemble your bank's website. Once you are there and enter your information, they have everything they need to access your real account and steal from you. You may even receive these kinds of email from banks/credit card companies where you do not hold accounts.

No financial institution will ever ask for your account information in an email. Never follow a link in a suspicious email. If you have to go to your bank's site, open a browser and type it in manually to check your account or any request they "seem" to be making of you. A lot of financial sites (like Paypal, for example) have a specific email account where you can send suspicious emails and they will tell you if it is real or not. If your institution does not have that type of email address available on their website, send the email to customer service and ask them if it is real or someone trying to scam you. Doing this keeps you from falling prey to this person and also alerts the financial institution that someone is trying to commit fraud on their customers.

**Bottom line: Be smart and safe. If you are unsure of what you are reading, do not click any links or give out any information. Call customer service or forward the email to your institution.**