



**FRONTIER  
BANK**

## Consumer Alert

This page is for the purpose of giving you the customer information to help protect you against the many fraudulent attempts of identity theft on the internet. Please be advised that Frontier Bank will never contact you via email for confidential information pertaining to you account(s) with us. It is the policy of Frontier Bank not to contact customers electronically. Email and the World Wide Web are not secure methods of contacting our customers. If you receive an email from us asking for sensitive information or to follow a link to update customer information please report the incident to us immediately at 866.216.0948 to report the email in question

\*Frontier Bank web site may contain links to other web sites operated by third parties. The linked sites are not under any control of Frontier Bank or its affiliates or subsidiaries, and Frontier Bank is not responsible for their content. Such links do not imply Frontier Bank's endorsement or guarantee of the products, information, or recommendations provided by any third party site. The third party site may have a privacy policy different from that of Frontier bank and may provide less security than the Frontier Bank web site. Frontier Bank disclaims all liability with regard to your access to such linked web sites. Frontier Bank provides links to other web sites as a service to users, and access to any other sites linked to Frontier Bank is at your own risk

### **Common Terms:**

*Definitions from Webopedia \* <http://www.webopedia.com>*

**Phishing** - (fish'ing) (n.) The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of

people, the “phisher” counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

- Federal Trade Commission Article How not to get hooked by a Phishing scam:  
<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.pdf> \*

**Pharming** - Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

**Spoofing** - Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP -- does not include a way to authenticate. There is an SMTP service extension (RFC 2554) that allows an SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information.

**Identity Theft** - For a resource of information about Identity Theft please visit the Federal Trade Commission website at the following address: <http://www.consumer.gov/idtheft/> \*