

CASE STUDY: How we helped a medium size bank

Recently, a phishing email and telephone scam targeted Litchfield Bancorp. Reacting decisively, Litchfield Bancorp responded through its fraud alert system. The bank's response included an internal email alert to all employees and warnings were posted about the fraud on its web site.

Litchfield Bancorp has always taken a proactive approach to fraud prevention. As an eFraud Prevention™ member, they were able to link the fraud alert directly to their consumer education portal (eFraud Prevention™). When consumers saw the warnings about the scams, they had the up-to-date resources to help them best understand how to avoid becoming a victim.

For the bank, this was a huge time saver. Litchfield Bancorp did not need to link to external sites or do research to find the right information regarding each type of fraud. They efficiently provided a comprehensive response that protected their customers from I.D theft and monetary losses.

ABOUT THE FRAUD

Phishing Scam: The phishing email was spam in nature and sent to a large group of random recipients. The fraudulent email had the Litchfield Bancorp logo and corporate color scheme. This information was easily obtained from its public Web site. The email displayed an online form and stated the following:

"Please confirm that you are the rightful owner of this account. Please fill out and submit the form below. This information is used for verification purposes only. We apologize for any inconvenience."

Telephone Scam: The criminals here made phone calls with bogus 'security alerts' that warned about a credit card data breach, stating that Litchfield Bancorp accounts may have been compromised and that personal information needs to be updated.

ABOUT LITCHFIELD BANCORP:

Litchfield Bancorp (assets 200 million) is a mutual savings bank with five locations in Connecticut. Visit them online at <http://www.litchfieldbancorp.com>