Bank of Botetourt

February 2026

A Consumer Scam Story: When a "Bank Alert" Wasn't from the Bank

How It Started
On a Tuesday morning, Linda, a long-time customer who regularly used mobile banking, received a text message that appeared to come directly from her bank. The message warned of "unusual debit card activity" and stated that her account would be temporarily restricted unless she verified the transaction immediately.

The text included a link and used language Linda recognized from past legitimate alerts. It arrived during her morning routine, when she was juggling work emails and personal responsibilities. Concerned about potential fraud, and wanting to act quickly, Linda clicked the link.

What Actually Happened
The link led to a website that closely resembled the bank's online banking login page, complete with familiar colors, logos, and formatting. Linda entered her username and password. Moments later, she received a one-time passcode on her phone and entered that as well, believing she was confirming her identity.

In reality, the website was controlled by scammers. As Linda entered her information, the criminals were using it in real time to access her actual bank account. With valid credentials and the one-time passcode, they bypassed security controls and gained full access.

Once inside the account, the scammers quickly changed contact details, added a new external payment method, and initiated several small

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

transactions designed to avoid triggering immediate alerts.

Linda did not realize anything was wrong until later that afternoon when she checked her balance and noticed transactions she did not recognize.

How It Was Resolved
Linda contacted her bank as soon as she noticed the suspicious activity. The bank's fraud team immediately restricted access to the account, blocked additional transactions, and began an investigation. Because the activity was reported quickly, several transactions were stopped before completion, and most of the funds were recovered.

The bank worked with Linda to reset her online banking credentials, review recent account activity, and set up additional alerts. She was also provided with education on identifying phishing messages and safely accessing online banking going forward.

While the experience was unsettling, quick action and communication helped limit the damage.

What You Should Do

- Do not click links in unexpected emails or text messages claiming to be from your bank
- Never share passwords or one-time passcodes with anyone
- Access online banking only through trusted apps or bookmarked websites
- Review account activity frequently
- Contact your bank immediately if you suspect fraud

Source: Article: OpenAI, ChatGPT, January 26, 2026
https://chatgpt.com/

A Business Scam Story: The Vendor Email That Changed Everything

How It Started
Mark, the controller for a small manufacturing company, managed vendor payments and cash flow as part of his daily responsibilities. One morning, he received an email from a long-standing supplier explaining that the vendor had changed banks and needed to update wire instructions for future payments.

The email appeared legitimate. It came from the vendor's real email address, referenced recent invoices, and used a tone consistent with prior correspondence. With multiple deadlines approaching and no obvious red flags, Mark updated the wire instructions in the accounting system and initiated a payment later that day.

What Actually Happened
Unknown to Mark, the vendor's email account had been compromised weeks earlier through a phishing attack.

Cybercriminals had been silently monitoring messages, learning the vendor's communication style and waiting for an opportunity to intervene.

When the timing was right, they sent the fraudulent "bank change" email. The wire instructions directed funds not to the vendor, but to an account controlled by the criminals. Once the wire was sent, the funds were quickly moved through multiple accounts to make recovery more difficult.

The issue only came to light several days later when the vendor followed up to ask why payment had not been received.

How It Was Resolved
Mark immediately contacted the bank upon realizing the mistake. The bank initiated a wire recall and filed appropriate notifications. Although only a portion of the funds could be recovered, the prompt response prevented additional losses.

Following the incident, the business worked closely with the bank to strengthen internal controls. New procedures were implemented, including mandatory call-back verification for payment changes, dual approval for wires, and employee training focused on business email compromise (BEC) scams.

The incident served as a costly but valuable lesson in how even trusted relationships can be exploited.

What You Should Do

- Verify all payment or account changes using a known, trusted phone number
- Never rely on email alone for wire or ACH instructions
- Implement dual controls and approval processes for payments
- Train employees regularly on phishing and social engineering risks
- Contact your bank immediately if fraud is suspected

Designed by Freepik

Source: Article: OpenAI, ChatGPT, January 26, 2026
https://chatgpt.com/