Bank of Botetourt

May 2026

Zelle® Scams on the Rise: What You Need to Know Before You Send Money

Peer-to-peer (P2P) payment services like Zelle® offer a fast and convenient way to send money, but that speed also makes them a growing target for scammers. Fraud involving Zelle has increased as criminals use sophisticated tactics to trick customers into sending money directly to them.

Understanding how these scams work is key to protecting your finances.

How the Scam Typically Works

Unlike traditional fraud, many Zelle scams involve authorized payments, meaning the customer is tricked into sending money themselves.

Common scenarios include:

- *Bank Impersonation Calls or Texts*
  Scammers contact you claiming to be from your bank's fraud department. They warn of suspicious activity and instruct you to send money to yourself or a "secure account" using Zelle. In reality, the funds are sent directly to the scammer.

- *Online Marketplace Scams*
  Fraudsters pose as buyers or sellers and request payment via Zelle. Once the payment is sent, the product or service never materializes.

- *Account "Verification" Scams*
  Victims are told they must send a Zelle payment to confirm or

Continued on page 2

EQUAL HOUSING LENDER

Member FDIC

Connect with us!

(540) 591-5000

protect their account. This is a tactic to move funds quickly out of your control.

Why Zelle Scams Are Effective

Zelle transactions are designed to be fast and final. Once money is sent, it is typically deposited within minutes and may be difficult to recover.

Scammers exploit:

- Urgency ("act now to stop fraud")
- Trust (impersonating your bank or known contacts)
- Confusion about how Zelle works

How to Protect Yourself

- Only send money to people you know and trust
- Never send money in response to an unexpected request
- Your bank will never ask you to send money to yourself or to a "safe" account
- Verify suspicious messages by contacting your bank directly using a trusted number
- Be cautious when using Zelle for online purchases or sales

Tips for Business Clients

Businesses should also be cautious when using Zelle or similar payment platforms:

- Avoid using P2P services for large or high-risk transactions
- Confirm payment requests independently before sending funds
- Educate employees on payment fraud and impersonation scams
- Use established payment controls for vendor transactions

If You Suspect Fraud

If you believe you've been targeted by a Zelle scam or may have sent money to a fraudster, it's important to act immediately. Contact us as soon as possible so steps can be taken to review the transaction and attempt recovery. You should also report the incident through your banking app or directly to Zelle, if applicable. The sooner fraud is reported, the greater the chance of minimizing potential losses.

Zelle is a fast, convenient, and secure way to send money to people you know and trust, but it is not intended for transactions with unknown parties or situations involving urgency or pressure. Taking a moment to pause, verify, and confirm before sending money can make a critical difference.

As your community bank, we are committed to helping you use digital payment tools safely and confidently. We encourage you to stay informed about emerging scams, monitor your accounts regularly, and reach out to us anytime you have questions or concerns about a transaction.

When it comes to protecting your financial information, a cautious approach and quick action are your best defenses.

Source: OpenAI, ChatGPT, April 20, 2026
https://chatgpt.com

Image: Wikipedia Commons

Business Email Compromise (BEC): A Growing Threat to Businesses of All Sizes

Business Email Compromise (BEC) remains one of the most financially damaging cyber threats facing businesses today. These scams are highly targeted, often difficult to detect, and designed to exploit trust within organizations.

For small and mid-sized businesses, the impact can be significant.

How BEC Scams Work

BEC scams typically begin with a compromised or spoofed email account. Fraudsters may impersonate:

- Company executives
- Employees
- Vendors or suppliers
- Trusted partners

They then send convincing emails requesting:

- Wire transfers
- Changes to payment instructions
- Sensitive financial or employee information

These requests often appear routine and may reference real invoices or ongoing transactions.

Why These Scams Are So Effective

BEC attacks rely on:

- Familiar communication patterns
- Timing (e.g., during busy periods or when key staff are unavailable)
- A sense of urgency or confidentiality

Because the request appears legitimate, employees may act quickly without verifying.

Warning Signs to Watch For

- Requests for urgent or unusual payments
- Changes to vendor payment details
- Emails that slightly alter a known address
- Pressure to bypass normal procedures
- Messages that insist on confidentiality

How to Protect Your Business

Strong internal controls are the most effective defense:

- Require dual approval for wire transfers and ACH payments
- Verify payment changes using a known, trusted phone number
- Implement multi-factor authentication (MFA) for email and financial systems
- Train employees regularly on fraud awareness
- Limit access to financial systems based on job roles

The Importance of Acting Quickly

If a fraudulent payment is suspected:

- Contact us immediately to initiate a recall
- Notify internal leadership and IT support
- Document the incident and preserve communications

Quick action can improve the chances of recovering funds.

A Shared Responsibility

Business Email Compromise is not just an IT issue; it is a financial and operational risk. By combining employee awareness with strong internal controls, businesses can significantly reduce their exposure.

We are here to support you with tools, education, and guidance to help protect your organization.

Source: OpenAI, ChatGPT, April 20, 2026
https://chatgpt.com