BANKNORTH | Protect Your Business

Business Email & Payment Fraud Prevention

Strengthen Authentication and Account Security

Enable Multi-Factor Authentication (MFA): Implement and enforce MFA on all accounts that support it, especially for email, financial, and administrative access.

Use Strong Passwords and Security Questions: Avoid easily guessed information such as pet names, birthdays, or family member details - these are often publicly available online.

Review Accounts Regularly: Activate text or email alerts through your financial institution and review bank statements regularly for suspicious activity.

Verify Requests and Payment Instructions

Verify Changes Through a Second Channel: Confirm account or payment changes using a verified phone number or separate communication method.

Be Wary of Urgent Requests: Fraudsters often pressure employees to act quickly. Slow down, verify, and escalate concerns to internal contacts such as legal or compliance teams.

Watch for Spoofing and Impersonation: Scammers often disguise caller IDs, email addresses, and URLs to look authentic. Examine details closely and verify authenticity before acting.

Call Back Using Known Contact Info: Never rely on contact details provided in suspicious emails, texts, or calls. Use a verified number from internal or public directories.

Establish Internal Controls

Set Dual-Approval Processes: Require multi-layer reviews or dual controls for transactions over specific thresholds. Define clear delegations of authority when approvers are unavailable.

Document and Train: Maintain written procedures for handling potential scams and ensure all employees are trained on how to recognize and respond appropriately.

Encourage Reporting: Create a culture where employees feel comfortable raising suspicions or verifying unusual requests before taking action.

Practice Safe Communication and Online Behavior

Think Before You Click: Avoid links or attachments in unexpected or unknown emails. Verify the sender and watch for suspicious requests, urgency, or unusual instructions.

Confirm Sensitive Communications: Before sharing confidential information, verify you're communicating with the intended person using a passphrase or other verification method.

Be Careful What You Share Online: Limit personal or company details shared on social media that could help scammers guess passwords or target your organization.

Stay alert, stay skeptical, and keep your business protected - always.