Protect Yourself from Imposter Scams

Fraudsters are constantly finding new ways to trick people into sharing personal and financial information. One common tactic is impersonation—pretending to be from a trusted organization, including your bank, to gain your trust.

Understanding how these scams work can help you recognize suspicious activity and protect your accounts.

Warning Signs of an Imposter Scam

Unsolicited "Great" Opportunities: Be cautious of unexpected offers or financial opportunities that sound unusually generous or urgent. Scammers often rely on enticing offers to get your attention.

Pressure to Act Immediately: Fraudsters may try to rush you into making quick decisions by claiming your account is at risk or that immediate action is required. Legitimate banks will give you time to verify requests and make informed decisions.

Unexpected Messages or Calls: If you receive a message, email, text, or phone call you did not initiate—especially from someone claiming to represent a financial institution—treat it with caution.

Requests for Sensitive Information or Device Access: Never share one-time passcodes, online banking credentials, or allow someone to remotely access your device. These requests are often attempts to gain control of your accounts.

Always Verify Before Sending Money

A common scam involves criminals sending emails that appear to come from a trusted vendor, client, or colleague requesting an ACH or wire transfer to a "new" account. In many cases, the email address is slightly altered or spoofed to look legitimate.

📞Before sending any payment or updating payment instructions, **always verbally verify the request using a trusted phone number you already have on file.** Do not rely on phone numbers or contact details included in the email or message requesting the change.

Taking a moment to confirm payment instructions can prevent costly fraud.

What to Do if Something Feels Suspicious

Pause: Do not share personal information or take action until you have verified the request through a trusted source.

Disconnect: End the conversation, close the message, or block the number or account contacting you.

Notify Us: If something does not feel right or you notice suspicious activity on your account, contact EagleBank immediately at 877.575.3245 or reach out to your local branch.

Please remember: EagleBank will never contact you through social media or messaging apps to request personal information or promote banking opportunities.

Your Security Matters

Protecting your financial information is a top priority for us. Staying alert and verifying requests—especially before sending ACH or wire transfers—can help safeguard your accounts. If you ever have questions or concerns, our team is here to help.