noabank
Good People, Smart Banking

Online Security Safety- Warning!

Banks do not ask for account numbers and other sensitive personal information by email.

If you have responded to a suspicious email, contact your bank immediately so it can protect your account and your identity.

Never give out your personal or financial information in response to an unsolicited phone call, fax or email, no matter how official it may seem. Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the email's validity using a telephone number or Web address you know to be genuine.

Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.

When submitting financial information online, look for the padlock or key icon at the bottom of your Internet browser. Most secure Internet addresses, though not all, use "https".

Report suspicious activity to the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx), a partnership between the FBI and the National White Collar Crime Center.

Notify us of any concerns at : help@noabank.com