URGENT ALERT - Major Uptick in Fraud and Scams

We want to ensure that you are well-informed about a significant increase in fraudulent activities and scams affecting individuals in our communities, as well as around the world. Scammers are using increasingly sophisticated methods to defraud people in a range of ways, and we don't want anyone to fall victim to these criminals. Please educate yourself on how to spot fraudulent behavior as your vigilance and proactive measures are essential in protecting yourself and your loved ones. Here are some important tips to avoid scams:

1. **Resist The Urge To Respond/React Quickly:** Scammers sometimes try to make you believe that something is rare or only available for a limited period. They urge victims to make a choice immediately rather than thinking about it or consulting with family, friends, or financial consultants. *If it seems too good to be true, it's likely too good to be true.*
2. **Safeguard Your Personal Information:** Never give out your personal information to someone who has approached you unexpectedly, whether by phone, email, social media, website, or even at your front door.
3. **Beware of Phishing Attempts:** Be cautious of unsolicited emails, text messages, and phone calls requesting personal or financial information. Always verify the authenticity of the source. Scammers are skilled at impersonation and just because a website, phone call, or email appears to be official, does not guarantee that it is official.
4. **Use Caution When Opening Attachments/Clicking Links:** Spamming emails are frequently used by cybercriminals to distribute viruses. When the virus (attachment/link) is opened and run, it can install itself in the background and begin its activity.
5. **Use Strong and Unique Passwords:** Create strong and unique passwords for your online accounts and consider changing them regularly. Do not share your passwords with anyone.
6. **Enable Two-Factor Authentication/Multi-Factor Authentication:** Add an extra layer of security to your online accounts whenever possible.
7. **Verify Requests for Sensitive Information:** Legitimate organizations will NEVER ask for sensitive information such as Social Security numbers, passwords, or financial details via email or phone.
8. **Monitor Your Financial Statements:** Regularly review your bank and credit card statements. Report any suspicious or unauthorized transactions immediately.
9. **Educate Yourself:** Be cautious of investment schemes or offers that seem too good to be true. Always verify the legitimacy of such opportunities. If you aren't expecting communication from a person or organization, it's always best to contact them directly before acting. Stay Informed and be aware of common scam tactics and stay updated on the latest fraud alerts and prevention tips.

If you come across ANY suspicious activity, please reach out to us immediately at 309/543-3361. Thank you for choosing Havana National Bank for your financial needs.

Sincerely,

Jeffery A. Bonnett

President/CEO