Bath Savings
Since 1852

FRAUD RED FLAGS

Bath Savings has many safeguards in place to protect your personal information. Still, it is important to be vigilant as fraud and identity theft scams are becoming more sophisticated every day.

- A person calls or emails, pretending to be someone you trust, such as a family member or a representative from your bank and asks for personal information such as a social security number or password. The person may threaten legal action or using intimidation tactics to get you to respond.
- You're asked to send money through undetectable methods such as wire transfers and gift cards, or they may even send a check and ask you to return some of the money through these methods.
- A person calls/emails and claims that you have won a sweepstakes. They tell you to send them money to cover taxes or processing fees.
- You receive a phone call from someone claiming to work for Microsoft who indicates they've noticed dangerous software on your computer. In order to triage this, they are requesting remote access to your computer. This is a scam.
- Phishers want you to click a link that allows them to install malware on your device or try to access secure information. A common scenario is delivery-related scams, often in the form of text/email that claims you have a lost package you can retrieve by clicking a link.
- Romance scammers create fake profiles on dating sites and social media. The scammers strike up a relationship with you to build up trust, then, they make up a story and ask for money. If the person you're chatting with can't meet in person and asks you for money, it's probably a scam.

If you believe your personal information may have been compromised, visit IdentityTheft.gov.

bathsavings.bank *800-447-4559* *MEMBER FDIC*

Bath Savings
Since 1852

PROTECT YOURSELF

While Bath Savings proactively monitors all of our accounts for suspicious activity 24/7, it's important that you stay vigilant in protecting yourself from fraud.

- Read your credit reports. You have a right to a free credit report every 12 months from *annualcreditreport.com* or by calling 1-877-322-8228.
- Set up Account Alerts in online banking to receive notifications of activity on your account.
- Check your bank, credit card, and account statements for mistakes.
- Shred all documents that show personal, financial, and medical information.
- Don't respond to email, text, and phone messages that ask for personal information.
- Never click on links or open attachments from unknown sources, and never give anyone you don't know remote access to your computer.
- Create complex passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- When shopping online, use websites that protect your information with encryption. An encrypted site has "https" at the beginning of the web address.
- Never share multi-factor security codes such as the four to eight-character codes you get through text message or email.
- Use anti-virus and anti-spyware software, and a firewall on your computer. Set automatic updates.
- Never send money to strangers (via wire, PayPal, Zelle, etc.) under any circumstances.

If you receive a suspicious email, call, or text, contact us at 800-447-4559 or bsi@bathsavings.bank.

We're here to help.