Financial Foundations – Powered by Newtown Savings Bank

Bank Impersonation Scams and Holiday Fraud

As the holiday season approaches, consumers are urged to stay vigilant against a surge in fraud schemes, particularly bank impersonation scams, which have become the most reported form of identity-related crime in 2025. According to the Identity Theft Resource Center (ITRC), impersonation scams rose by a staggering 148% over the past year, with 21% of these scams involving criminals posing as financial institutions.

Understanding Bank Impersonation Scams

Bank impersonation scams typically involve fraudsters contacting individuals via phone, email, or text, pretending to be representatives from legitimate banks. These scammers often use spoofed phone numbers, official-looking emails, or fake websites to convince victims to share sensitive information such as account numbers, passwords, or Social Security numbers. Once obtained, this data is used to take over accounts or create new fraudulent ones.
The ITRC reports that 53% of identity misuse cases involved account takeovers, while 36% involved the creation of new accounts using stolen personal information. Financial accounts remain the primary target, with credit cards (56%) and checking accounts (14%) being the most affected.

Holiday Season: Prime Time for Scammers

The holiday season traditionally sees an uptick in fraud, as consumers increase online shopping, travel bookings, and charitable donations. Scammers exploit this busy period by launching phishing campaigns, fake charity solicitations, and package delivery scams.

Artificial intelligence is also fueling the rise in fraud. Criminals now use AI to generate realistic fake customer service interactions, clone voices, and create convincing phishing websites, making it harder for consumers to detect deception.

How to Protect Yourself

You can take several steps to safeguard your personal and financial information:

- **Verify**: If you receive a call, email, or text claiming to be from your bank, do not respond directly. Instead, contact your bank using a verified phone number or website.
- **Enable multi-factor authentication**: This adds an extra layer of security to your accounts.
- **Monitor your accounts regularly**: Look for unfamiliar transactions and report suspicious activity immediately.
- **Be cautious with payment apps**: Only send money to people you know and trust.

For more information on how to protect yourself from fraud, visit www.nsbonline.com/security-and-privacy.