Bank of Botetourt

March 2026

National Slam the Scam Day & National Consumer Protection Week

Member FDIC

EQUAL HOUSING LENDER

March is nationally recognized as an important month for fraud awareness and consumer education. In 2026, **National Consumer Protection Week will take place March 1–7**, with **National Slam the Scam Day observed on Thursday, March 5, 2026**.

These initiatives are designed to educate individuals and businesses about fraud prevention, identi protection, and financial security. While these awareness efforts occur during a single week, the lessons they promote are relevant year-round.

As your community bank, we believe education is one of the strongest defenses against financial fraud. Taking time to understand today's most common scams, and the controls that prevent them can significantly reduce risk for both households and businesses.

Understanding the Purpose of These Awareness Initiatives
National Consumer Protection Week (NCPW) focuses broadly on empowering consumers with knowledge about fraud prevention, deceptive practices, identity theft, and reporting resources. The goal is simple: informed customers are harder to scam.

National Slam the Scam Day, observed during NCPW, places special emphasis on imposter scams. These schemes occur when criminals pose as trusted organizations, such as financial institutions, government agencies, utility companies, or even local businesses, to trick victims into sharing sensitive information or sending money.

Both initiatives emphasize three key principles:

1. Pause before responding to unexpected requests
2. Verify independently using trusted contact information
3. Report suspicious activity immediately

What This Means for Personal Banking Customers
Individuals remain frequent targets of fraud because cybercriminals often rely on emotional triggers—fear, urgency, curiosity, or excitement—to override caution.

Common Scams Targeting Consumers
Imposter Bank Alerts
Fraudsters send texts or emails claiming there is suspicious activity on your account. The message urges you to click a link or call a number immediately. The link often leads to a fake website designed to capture login credentials.

Government or Law Enforcement Scams
Scammers claim you owe taxes, face legal consequences, or must verify personal information immediately. They may demand payment via wire transfer, gift cards, or cryptocurrency.

Connect with us!

(540) 591-5000

Continued on page 2

Account Takeover Attempts
Criminals obtain login credentials through phishing or data breaches and attempt to access online banking accounts.

Romance and Investment Scams
Fraudsters build trust over time and eventually request financial assistance or promote fraudulent investment opportunities.

How Consumers Can Protect Themselves
National Consumer Protection Week serves as a reminder to evaluate your personal security practices:

- Never share passwords or one-time authentication codes
- Access online banking only through official apps or bookmarked websites
- Be skeptical of urgent or threatening messages
- Review account activity regularly
- Set up transaction alerts for real-time monitoring

Most importantly, contact us immediately if you suspect fraud. Prompt reporting increases the likelihood of stopping or recovering unauthorized transactions.

What This Means for Business Banking Customers
While consumers face daily phishing and imposter attempts, businesses are increasingly targeted with sophisticated fraud schemes that can result in substantial financial losses.

Small and mid-sized businesses are especially attractive targets because criminals perceive them as having financial access but fewer layered security controls than larger corporations.

Common Scams Targeting Businesses
Business Email Compromise (BEC)
Fraudsters gain access to a legitimate email account, either yours or a vendor's, and use it to request wire transfers or payment changes.

Vendor Payment Redirection Fraud
A criminal impersonates a vendor and sends "updated" wire instructions. Funds are unknowingly transferred to fraudulent accounts.

Payroll Diversion Schemes
Scammers pose as employees and request direct deposit changes.

Ransomware Attacks
Malicious software encrypts company data and demands payment for restoration.

How Businesses Can Strengthen Their Defenses
National Slam the Scam Day is an ideal opportunity for businesses to review internal controls and operational safeguards.

Key risk mitigation practices include:

- Implementing dual authorization for wire and ACH transactions
- Requiring call-back verification for payment or account changes
- Enabling multi-factor authentication for online banking and email systems
- Conducting regular employee training on phishing and social engineering
- Limiting system access based on job responsibilities
- Maintaining secure, tested data backups

Cybersecurity is no longer solely an IT function; it is a core component of operational resilience and financial risk management.

The Importance of Acting Quickly
Whether you are a consumer or business owner, time is critical in fraud situations.

If suspicious activity is identified:

1. Contact us immediately
2. Do not attempt to "fix" the situation independently
3. Preserve any suspicious communications
4. Follow guidance from your us and, if necessary, law enforcement

Early reporting significantly improves the possibility of limiting losses.

How Your Community Bank Supports You
Fraud prevention is a partnership. While awareness initiatives highlight the importance of vigilance, we work year-round to help safeguard your accounts.

We encourage all customers, personal and business alike, to use National Consumer Protection Week as a time to:

- Review account security settings
- Update passwords
- Confirm multi-factor authentication is enabled
- Revisit internal payment controls
- Educate family members or employees about current scams

Awareness Is the First Line of Defense
Scammers continually evolve their tactics. However, most fraud attempts still rely on predictable strategies: urgency, impersonation, and pressure.

National Consumer Protection Week (March 1–7, 2026) and National Slam the Scam Day (March 5, 2026) serve as timely reminders that staying informed is one of the most effective ways to protect your finances.

If you ever have questions about a suspicious message, phone call, or transaction, please contact us directly using a trusted phone number or visit our official website. When it comes to protecting your financial well-being, it is always better to pause and verify.

Source: OpenAI, ChatGPT, February 23, 2026
https://chatgpt.com

SLAM THE SCAM

Securing Your Home Network: Best Practices for Protecting Your Financial Information

Your home Wi-Fi network connects everything from smartphones and laptops to smart TVs and security systems. While convenient, this connectivity also creates potential entry points for cybercriminals. An unsecured home network can expose online banking credentials, stored payment information, personal data, and even business systems accessed remotely.
Taking a few proactive steps can significantly reduce your risk.

1. Change Default Router Settings
Many routers come with default administrator usernames and passwords that are widely known.

- Change the router's login credentials immediately.
- Use a strong, unique passphrase.
- Avoid reusing passwords from other accounts.

2. Use Strong Encryption and a Secure Wi-Fi Password
Ensure your router is using current encryption standards (WPA3 or WPA2).

- Avoid outdated security settings such as WEP.
- Create a complex Wi-Fi password and do not share it broadly.
- Consider setting up a separate guest network for visitors.

3. Keep Your Router and Devices Updated
Outdated software is a common vulnerability.

- Install router firmware updates when available.
- Keep computers, phones, and apps updated.
- Use reputable antivirus or endpoint protection software.

4. Enable Multi-Factor Authentication (MFA)
Even if login credentials are compromised, MFA adds an additional layer of protection.

- Enable MFA for online banking, email, and financial apps.
- Set up account alerts to monitor transactions in real time.

5. Protect Remote Work and Business Access
If you access business banking or company systems from home:

- Use a secure, company-approved VPN when required.
- Keep work devices separate from personal devices.
- Implement dual approvals for financial transactions whenever possible.

6. Monitor for Warning Signs
Be alert for:

- Unknown devices connected to your network
- Changes to router settings you did not make
- Unexpected password reset notifications
- Unusual account activity

If you suspect your financial information may be compromised, contact us immediately.

A secure home network is one of the most important foundations of financial protection.

While we employ strong safeguards to protect your accounts, cybersecurity is most effective when customers take proactive steps at home.

If you have questions about securing your accounts or notice suspicious activity, please contact us directly using a trusted phone number or our official website. We are here to help you bank safely and confidently.

Source: OpenAI, ChatGPT, February 23, 2026
https://chatgpt.com

Designed by Freepik