Bank of Botetourt

January 2026

Cybersecurity Is a Shared Responsibility

At our bank, protecting your financial information is one of our highest priorities. We invest in advanced security technologies, continuous monitoring, and layered safeguards designed to protect your accounts and transactions. These measures operate around the clock to help detect and prevent unauthorized activity. At the same time, cybersecurity is most effective when customers are informed, engaged, and cautious in their day-to-day digital activity.

Cybercriminals today rarely rely on technical hacking alone. Instead, many attacks focus on deceiving individuals into providing information voluntarily. Phishing emails, fraudulent text messages, and impersonation phone calls are designed to look legitimate and often create a sense of urgency, such as a warning about account access, a suspicious charge, or an unexpected payment request. These messages may appear to come from a bank, vendor, employer, or even a known contact.

We encourage our customers to slow down and carefully evaluate unexpected requests. Legitimate organizations, including our bank, will never ask you to share sensitive information such as online banking credentials, full account numbers, or one-time security codes through email or text messages.

To help protect yourself, we recommend the following best practices:

- Be cautious of unsolicited emails, texts, or phone calls requesting personal or financial information
- Avoid clicking links or downloading attachments from unfamiliar or suspicious messages
- Verify unusual requests by contacting the sender using a trusted phone number or website you already know
- Use strong, unique passwords for online banking, email, and other important accounts
- Enable multi-factor authentication whenever it is available

It is also important to keep your devices secure. Using up-to-date software, antivirus protection, and secure internet connections reduces the risk of unauthorized access. If you notice unusual account activity or believe your information may have been compromised, contact us promptly so we can assist.

Cybersecurity is not just about technology — it is about awareness, communication, and shared responsibility. By staying informed and taking simple precautions, you help protect not only your own accounts, but the broader financial community as well. We are committed to partnering with you to keep your financial information safe.

Source: Article: OpenAI, ChatGPT, December 23, 2025 https://chatgpt.com/

Continued on Page 2

EQUAL HOUSING LENDER Member FDIC

Connect with us!

(540) 591-5000

Protecting Your Home Network Helps Protect Your Finances

Many of today's financial activities — including online banking, paying bills, managing investments, and running a business — take place over home internet connections. Because of this, the security of your home network plays an important role in protecting your personal and financial information. A secure home network helps reduce the risk of unauthorized access to your devices and online accounts.

Home Wi-Fi networks are often targeted because they can be overlooked or left with default settings. An unsecured or poorly configured network can allow cybercriminals to intercept data, install malicious software, or gain access to connected devices. Once inside a home network, attackers may attempt to capture passwords, monitor activity, or access financial accounts.
Fortunately, a few simple steps can significantly strengthen your home network security.

We recommend that customers:

- Change the default username and password on your Wi-Fi router, as default settings are widely known and easily exploited
- Use a strong, unique Wi-Fi password and enable modern encryption, such as WPA2 or WPA3
- Keep your router's firmware and all connected devices updated with the latest security patches
- Use antivirus and security software on computers and mobile devices
- Avoid accessing sensitive accounts, including online banking, over public Wi-Fi networks

For households with multiple users, smart devices, or home offices, consider creating a separate guest network. This helps limit exposure by keeping personal devices and financial activity separate from less secure or shared devices.

It is also important to remember that every connected device — from smartphones and laptops to smart TVs and home assistants — becomes part of your network. Reviewing device settings and removing devices you no longer use can further reduce risk.

Taking these precautions helps create a safer online environment for managing your finances. If you have questions about protecting your accounts or notice suspicious activity, please contact us promptly. We are committed to helping you safeguard your financial information and use digital banking services with confidence.

Source: Article: OpenAI, ChatGPT, December 23, 2025 https://chatgpt.com/

Cybersecurity Guidance for Our Business Customers

Small businesses are the backbone of our community, and we are committed to supporting your success. Unfortunately, cybercriminals increasingly target small and midsize businesses, often assuming they have fewer security resources or less formal controls in place.

A cyber incident, such as a phishing scam, ransomware attack, or fraudulent payment request, can disrupt operations, compromise sensitive data, and result in financial loss. Even a single incident can have long-lasting effects on a business.

We encourage our business customers to:

- Train employees to recognize phishing emails, fake invoices, and social engineering tactics
- Use multi-factor authentication for online banking, email, and remote access systems
- Limit employee access to systems and data based on job responsibilities
- Back up critical business data regularly and store backups securely
- Establish clear procedures to verify wire transfers, ACH payments, and payment changes

Cybersecurity is not just an IT concern — it is a core business risk management issue. We view security as a shared responsibility and are committed to partnering with you to help protect your business and financial relationships.

Source: Article: OpenAI, ChatGPT, December 23, 2025 https://chatgpt.com/
Image: Freepik, Freepik Terms of Use

Designed by Freepik

Staying One Step Ahead of Cyber Fraud

Cyber fraud continues to evolve, and criminals are constantly finding new ways to exploit trust, technology, and routine processes. While our bank uses multiple layers of security to help protect your accounts, awareness remains one of the most effective tools in preventing fraud before it happens.

Many fraud attempts today rely on impersonation. Criminals may pose as a bank representative, vendor, employee, or even a familiar contact. These communications often appear legitimate and may reference real names, logos, or recent activity. The goal is usually to prompt quick action, such as confirming account details, approving a payment, or sharing a one-time security code.

One of the most important things you can do is slow down. Urgency is a common red flag. Requests that pressure you to act immediately, bypass normal procedures, or keep the request confidential should be treated with caution.

When in doubt, take the extra step to verify the request using a phone number or website you already trust.

We encourage our customers to keep the following principles in mind:

- We will never ask for your online banking password or one-time security codes
- Unexpected requests to move money, change payment instructions, or share sensitive information should always be verified
- Fraudulent messages often contain subtle signs, such as unusual wording, unfamiliar sender addresses, or requests outside normal processes

For business customers, internal controls are especially important. Separating duties, requiring secondary approvals for payments, and confirming changes to vendor instructions can significantly reduce risk. Even simple verification steps can prevent costly losses.

If you believe you have received a suspicious message or notice unusual account activity, contact us as soon as possible. Early reporting allows us to take quick action and help protect your accounts.

Cybersecurity is an ongoing effort, and threats will continue to change. We are committed to providing secure banking services and practical guidance to help you stay informed and protected. By remaining vigilant and working together, we can reduce risk and help keep your financial information secure.

Source: Article: OpenAI, ChatGPT, December 23, 2025 https://chatgpt.com/
Image: Freepik, Freepik Terms of Use

Designed by Freepik