Bank of Botetourt

September 2026

Fall Into Better Cybersecurity Habits: A Checkup for Your Financial Security

Member FDIC

EQUAL HOUSING LENDER

September is a natural time to get back into a routine. Students are back in school, summer travel is winding down, and businesses are preparing for the final months of the year. It is also a good time to take a few minutes to review your cybersecurity habits and make sure your financial information is protected.

As your community bank, we want to help you recognize potential risks and take simple steps to protect your accounts, whether you bank with us personally or manage your business finances with us.

Start With Your Financial Accounts

Your banking and financial accounts contain some of your most sensitive information. Take a few minutes to review your security settings and account activity.

Make sure you are:

- Using strong, unique passwords
- Enabling multi-factor authentication (MFA) when available
- Keeping your contact information current
- Reviewing your account activity regularly
- Setting up account and transaction alerts

If you see a transaction or login you don't recognize, don't wait to investigate. Contact us as soon as possible using a trusted phone number.

Connect with us!

(540) 591-5000

Continued on page 2

Give Your Devices a Security Checkup

Your computer, smartphone, and tablet are often the gateway to your financial accounts. Make sure your operating system, apps, web browser, and security software are current.

It's also a good time to remove apps and programs you no longer use. The fewer unnecessary applications on your devices, the fewer potential opportunities there are for cybercriminals.

Be Alert to Phishing Attempts

As routines become busier, it's easy to react quickly to an email or text message without stopping to consider whether it's legitimate.

Be especially cautious of messages claiming to involve:

- Suspicious activity on your bank account
- Password or account verification
- Package deliveries
- Payment requests
- School, employer, or financial information

Remember, scammers often create a sense of urgency to get you to act before you have time to think. If you receive a message that appears to be from us and you're unsure whether it's legitimate, don't click the link or provide information. Contact us directly using a trusted method.

A Reminder for Our Business Customers

For our business banking customers, September is also an excellent time to review your company's financial controls before entering the final quarter of the year.

Consider whether your business has appropriate procedures for:

- Approving ACH and wire transactions
- Verifying changes to vendor payment instructions
- Protecting online banking and email accounts with MFA
- Training employees to recognize phishing and payment fraud
- Reviewing user access to financial systems

A simple verification procedure can make a significant difference. For example, a request to change a vendor's account information should be independently confirmed using a known phone number, not the contact information included in the request.

Make Security Part of Your Routine

Cybersecurity doesn't have to be complicated. Strong passwords, MFA, account monitoring, careful handling of unexpected messages, and good financial controls can go a long way toward protecting you from fraud.

As your community bank, we're here to help you protect your financial information. If something doesn't look right or you're unsure about a request involving your account, stop and contact us before taking action. We'd rather have you ask a question than discover that a scammer got there first.

Source: OpenAI, ChatGPT, August 13, 2026
Image Attribution: Image by vectorjuice on Magnific

Is That Really Your Bank Calling?
How to Recognize Customer Service Scams

Imagine receiving a phone call from someone who says they're calling from your bank. The caller tells you there has been suspicious activity on your account and that they need to verify some information immediately.

They know your name. They may even know the last four digits of your account or debit card. The caller sounds professional and gives you a phone number or instructions for "securing" your account.

It sounds convincing, but it could be a scam.

Fraudsters are increasingly impersonating banks and other trusted organizations in an effort to obtain customers' financial information or convince them to move money. Understanding how these scams work can help you recognize the warning signs.

How the Scam Works

The scam often begins with an unexpected phone call, text message, or email claiming there is a problem with your account. The fraudster may tell you that someone is attempting to access your account or that a transaction needs to be verified.

The scammer may then ask you to provide:

- Your online banking username or password
- A one-time authentication code
- Your debit or credit card information
- Personal identifying information
- Money through a transfer or payment

The request may sound reasonable because the scammer is creating a sense of urgency.

Don't Trust Caller ID Alone

Caller ID is not proof that a call is legitimate. Fraudsters can manipulate the information displayed on your phone to make a call appear to come from a bank or another trusted organization.

If you receive an unexpected call about your account, you don't have to stay on the phone. Hang up and contact us directly using the phone number on the back of your debit card, your bank statement, or our official website.

Never Give Someone Your One-Time Authentication Code

One-time authentication codes are designed to protect your account. If someone unexpectedly contacts you and asks for a code that was just sent to your phone or email, stop.

The person may be attempting to use that code to gain access to your account. Never assume that someone is legitimate simply because they know some of your personal information.

Our Business Customers Need to Be Alert, Too

These same tactics can be used against businesses. A fraudster may impersonate a bank employee, company executive, vendor, or technology provider and request an urgent payment or change to account information.

We encourage business customers to establish procedures requiring employees to independently verify unusual requests involving wires, ACH transactions, vendor information, or sensitive data.

For example, if an employee receives an email requesting a change to a vendor's payment instructions, the employee should call the vendor using a previously established phone number, not a number provided in the email.

When in Doubt, Stop and Verify

Scammers want you to act quickly. We want you to **take your time.**

If you receive an unexpected communication about your account, stop before providing information, sending money, or clicking a link. Contact us through a trusted method and let us help you determine whether the request is legitimate.

And remember: you will never be inconveniencing us by asking whether something is a scam. When it comes to protecting your money, it's always better to pause and verify.

If you believe you have provided information to a fraudster or notice suspicious activity on your account, contact us immediately. The sooner we know about a potential problem, the sooner we can help.

Source: OpenAI, ChatGPT, August 13, 2026