Bank of Botetourt

November 2025

Building a Cyber-Strong Community: Takeaways from Cybersecurity Awareness Month

October was Cybersecurity Awareness Month, and while the month may be over, the lessons we learned are worth carrying forward all year long.

At Bank of Botetourt, your security is at the heart of everything we do. Whether you're checking your balance on your phone, managing payroll for your business, or sending money to a family member, cybersecurity plays a vital role in keeping your information and finances safe.

This year's national theme, "Building a Cyber Strong America," highlighted a simple but powerful truth: *cybersecurity isn't just for large organizations or IT experts. It's something we all share responsibility for—individuals, families, and businesses alike.*

The "Core Four" of Cyber Safety
This year, experts across the country emphasized four fundamental habits that dramatically reduce cyber risk. Think of them as the "seatbelts" of your digital life: simple, reliable, and proven to keep you safer.

1. **Use strong passwords**
   Weak or reused passwords are one of the biggest reasons accounts are compromised. Use long, complex passwords that include letters, numbers, and symbols—and avoid reusing them across multiple sites. Password managers can safely store and generate them for you.
2. **Turn on multi-factor authentication (MFA)**
   MFA adds a second step—like a code sent to your phone—when logging in. It's one of the easiest and most effective ways to stop hackers, even if they get your password. We strongly recommend enabling MFA wherever possible, especially for banking, email, and business systems.
3. **Recognize and report scams**
   Phishing remains one of the most common threats. Cybercriminals are getting more sophisticated, using fake emails, texts, or even phone calls that

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

look and sound legitimate. Remember:

- We will never ask you to share your online banking password or verification codes.
- Be cautious of urgent messages that pressure you to act immediately or click a link.
- When in doubt, contact us directly using the phone number on our website or your bank statement.

4. **Keep software and devices updated**
   Updates often contain security patches that fix known vulnerabilities. Whether it's your phone, computer, router, or banking app—keeping software current is one of the simplest ways to stay protected.

The Threats Are Changing—Here's What to Watch
Cybercriminals are always adapting, and this year's campaign highlighted how new technologies have changed the threat landscape.

- **Artificial intelligence (AI)** is being used to craft highly realistic scams, including fake voice messages ("vishing") and emails that sound just like someone you know.
- **QR code phishing ("quishing")** has become more common—attackers replace legitimate QR codes with malicious ones that lead to fake websites.
- **Business email compromise** is still one of the most damaging types of fraud, especially for small and midsize businesses. Scammers pose as trusted vendors, executives, or even bank representatives to request urgent wire transfers or payment changes.

For individuals, that might mean being cautious about unexpected messages, even from people you know. For business customers, it's critical to verify requests before sending payments or sharing sensitive data. A quick phone call to confirm can prevent a costly mistake.

Your Cybersecurity Checkup
Here's a quick list to help you put these lessons into action:

- ✓ Review and update your passwords.
- ✓ Turn on MFA for your online banking, email, and social media accounts.
- ✓ Update your devices and apps.
- ✓ Back up your important files securely.
- ✓ Be cautious of any message asking for personal or financial information.
- ✓ If something feels off, contact us directly before responding or taking action.

For businesses:

- ✓ Confirm any payment or vendor changes through a second channel, such as a verified phone call.
- ✓ Review internal controls and separation of duties for handling funds.
- ✓ Ensure employees receive regular cybersecurity training.

Staying Cyber-Smart, Together
Cybersecurity Awareness Month reminds us that we're all part of a connected system. The safer you are online, the safer our entire community becomes.

At Bank of Botetourt, we're committed to helping you stay informed, alert, and protected. Whether you're an individual customer or a business client, we're always here to answer questions or help you take additional steps to secure your accounts.

If you ever notice suspicious activity or want to learn more about how to protect your information, please reach out to your local branch or visit our Education Center on our website.

Together, we can keep our community and your finances safe and secure.

Sources/Credit:
Article: OpenAI, ChatGPT, October 23, 2025, https://chatgpt.com/
Image: Freepik; Freepik Terms of use

Designed by FreePik

Think Before You Dial:
Fake Phone Numbers in Online Searches

Scammers have found a new way to trick people by posting fake customer service numbers in online search results.

When you search Google for a company's phone number, you might see what looks like a real result—but it could connect you to a scammer instead.

What's happening?
Criminals are manipulating search listings and even real websites to display fraudulent phone numbers. You might think you're calling your bank, airline, or favorite retailer but instead, you're speaking with someone who wants your personal or financial information.

Some scammers even use AI tools to make fake listings or "AI Overview" results look more convincing.

What They're After
Once you're on the phone, the scammer may:

- Ask for your account number, password, or one-time security codes
- Request remote access to your computer or phone
- Urge you to "verify" recent transactions or move money to a "safe" account

These are all red flags. No legitimate company will ever ask for that kind of sensitive information over the phone.

Here's a summary of how this scam works, with real-world examples:

- Scammers pay for or manipulate search results so that when you look up a company's customer support number, you may end up calling a fraudulent number rather than the real one. For example, tech-support scammers have hijacked the help pages of legitimate brands — you might see what appears to be a genuine page for a company like Apple or Netflix, but the phone number shown is controlled by a scammer. Malwarebytes+1

- In one case, a consumer in New Jersey searched for a customer service number for a retailer via Google, found a number, called it and the person on the line asked for banking and personal info. CBS News

- Another dimension: in some search results, major companies' sites are technically real, but scammers have injected fake numbers into pages via manipulated URLs so you remain on the "legit" site while seeing the wrong number. Malwarebytes

- Additionally, search engine "AI Overviews" (prompts at the top of search results) and auto filled "help numbers" are being exploited—false contact numbers build up credibility and can become top-ranked

How to Protect Yourself
- **Use official websites** — Go directly to a company's site or your past statement for verified contact numbers.
- **Be cautious with search results** — Don't assume the first number you see online is correct.
- **Hang up if something feels off** — Then call back using a known, official number.
- **Businesses:** Keep a verified list of vendor and partner contact numbers and train employees to confirm changes through trusted channels.

A Final Reminder
Scammers count on quick reactions and misplaced trust. Taking a moment to verify a phone number before calling could save you from serious financial loss.

If you ever have doubts about a call or message claiming to be from Bank of Botetourt, hang up and call us directly using the number on your statement or our official website.

Your security is our priority; every call, every time.

Sources/Credit:
Article: OpenAI, ChatGPT, October 23, 2025, https://chatgpt.com/
Image: Freepik; Freepik Terms of use

Designed by FreePik