Bank of Botetourt

October 2026

Cybersecurity Awareness Month: Protecting What Matters Most

October is Cybersecurity Awareness Month, making it a good time to take a closer look at how we protect our personal and financial information. While cybersecurity often brings to mind passwords, firewalls, and antivirus software, one of the most important parts of security is something much simpler: people.

As your community bank, we take the security of your financial information seriously. We also know that today's scams often rely less on breaking through technology and more on convincing someone to trust a message, click a link, share information, or send money.

Scammers Use Trust and Urgency
Cybercriminals know that people are more likely to make a mistake when they feel rushed, worried, or pressured. A scammer may impersonate your bank, a family member, a business partner, a vendor, or another trusted organization.

You may receive a message claiming that:

- Suspicious activity has been detected on your account.
- Your payment or account needs immediate attention.
- A password or account needs to be verified.
- A family member needs money urgently.
- A vendor has changed its payment information.
- An employee or executive needs an urgent wire or ACH payment.

Continued on page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

These messages can look and sound legitimate. That is why one of the best defenses is simply to slow down.

Stop, Think, and Verify
Before clicking a link, providing information, or sending money, ask yourself:

- *Was I expecting this request?*
  If not, take a moment before responding.

- *Does the request make sense?*
  Be especially cautious when someone suddenly asks for sensitive information or a financial transaction.

- *Can I verify it another way?*
  Instead of replying to the message or using the phone number provided, contact the person or organization directly using a trusted phone number or other known method.

If someone contacts you claiming to be from your bank, remember that you should never provide your online banking password or a one-time authentication code in response to an unexpected request. If you are unsure whether a call, text, or email is legitimate, contact us directly using a trusted number.

Businesses Face the Same Risks
For our business customers, these same tactics can lead to significant financial losses. A convincing email from a vendor requesting a change to payment instructions, or an urgent request for a wire or ACH transaction, may not be what it appears to be.

Make independent verification part of your normal process. Confirm payment changes and unusual financial requests using a known phone number or another trusted method. Businesses should also use multifactor authentication, limit access to financial systems, regularly review user permissions, and provide employees with ongoing security awareness training.

Make Cybersecurity a Daily Habit
Cybersecurity Awareness Month is a great reminder that protecting your information does not have to be complicated. Strong, unique passwords, multifactor authentication, current software, and careful attention to unexpected requests can go a long way toward protecting your accounts.

Most importantly, give yourself time to think. Scammers want you to act quickly. Taking a moment to stop and verify a request can make all the difference.

As your community bank, we are here to help. If something seems suspicious or you are unsure whether a request is legitimate, contact us before taking action. We would much rather answer your question than have you take an unnecessary risk with your information or your money.

Article Source: OpenAI, ChatGPT, September 23, 2026
Image Source: OpenAI, ChatGPT, September 23, 2026

Don’t Let Ghost Accounts Haunt You: Cleaning Up Your Digital Life

Halloween is a good time for scary stories; but there’s one kind of “ghost” you probably don’t want following you around: old digital accounts and forgotten access.

Over the years, most of us accumulate online accounts we no longer use. Maybe it’s an old shopping account, a forgotten subscription, an email address you stopped using, or an app you downloaded once and never opened again. These accounts may seem harmless, but they can create unnecessary security risks if they remain active.

Those Old Accounts May Still Be Connected
A forgotten account may still contain personal information, saved payment details, or access to an email address. If you reused a password from that account somewhere else, a compromised account could potentially put other accounts at risk.

Take some time this fall to identify accounts you no longer need. If an account is no longer being used, consider closing it and removing stored payment information.

While you're cleaning house, check the apps connected to your important accounts. Remove access for apps and services you no longer use, particularly those connected to your email or financial information.

Businesses Have Digital Ghosts, Too
For businesses, forgotten access can be an even bigger concern.

Former employees, outdated vendor accounts, unused software, and old administrative credentials can remain active long after they are needed. Each unnecessary account or permission creates another potential entry point into your business systems.

Business owners and managers should periodically review:

- *Employee access*
  Remove accounts and access promptly when employees leave or change roles.
- *Administrative privileges*
  Limit elevated access to employees who actually need it.
- *Third-party access*
  Review applications, vendors, and services that have access to business systems or data.
- *Old accounts*
  Disable accounts that are no longer needed.
- *Passwords and authentication*
  Make sure important accounts use strong, unique passwords and multifactor authentication.

Give Your Digital Life a Fall Cleaning
You don't need to wait for something suspicious to happen before cleaning up your digital accounts. A few minutes spent reviewing what you have, and what you no longer need, can reduce your digital exposure.

Think of it as a cybersecurity version of cleaning out the attic: if you don't use it, don't need it, and don't know why it's still there, it's probably time to get rid of it.

This Halloween, don't let forgotten accounts become digital ghosts. Take a few minutes to review your online accounts, apps, and access permissions. A cleaner digital footprint can mean fewer places for trouble to hide.

Article Source: OpenAI, ChatGPT, September 23, 2026
Image Source: OpenAI, ChatGPT, September 23, 2026