Bank of Botetourt

August 2026

Back-to-School, Back to Scams: How to Stay Safe During the Busy Shopping Season

August is one of the busiest shopping months of the year. Families are purchasing school supplies, clothing, electronics, and other essentials, while businesses are preparing for increased activity heading into the fall. Unfortunately, scammers know this and often use the back-to-school season to target unsuspecting consumers.

Whether you're shopping online or in stores, taking a few extra precautions can help protect your personal and financial information.

Watch Out for Fake Online Stores
Cybercriminals often create websites that look like legitimate retailers and advertise deep discounts on popular back-to-school items. Once an order is placed, the merchandise never arrives—or worse, your payment information is stolen.

Before making a purchase:

- Shop with retailers you know and trust.
- Look carefully at the website address for misspellings or unusual domain names.
- Be cautious of deals that seem too good to be true.
- Research unfamiliar sellers before purchasing.

Beware of Phishing Emails and Text Messages
Scammers may send fake shipping notifications, discount offers, or coupons designed to get you to click on malicious links.
Instead of clicking links in emails or text messages:

- Visit the retailer's website directly.
- Track packages using official shipping company websites or apps.

Continued on page 2

EQUAL HOUSING LENDER

Member FDIC

Connect with us!

(540) 591-5000

- Never provide login credentials or payment information through unsolicited messages.

Use Secure Payment Methods
Whenever possible:

- Use a credit card or trusted digital payment service.
- Avoid sending money through person-to-person payment apps when purchasing from someone you don't know.
- Monitor your accounts regularly for unauthorized transactions.

Tips for Business Customers
Businesses preparing for seasonal purchasing should also remain vigilant. Fraudsters often impersonate vendors or shipping companies during busy buying periods.

Verify changes to payment instructions through a known phone number, and ensure employees responsible for purchasing understand the warning signs of phishing and payment fraud.

Shop Smart This School Year
The excitement of preparing for a new school year shouldn't come with the risk of financial fraud. Taking a few moments to verify websites, monitor your accounts, and think before you click can help ensure your back-to-school shopping season is safe and successful.

Source: OpenAI, ChatGPT, July 23, 2026

Protecting Your Digital Life: Why Every Household Needs a Cybersecurity Plan

Most families have plans for emergencies like severe weather or medical situations, but few think about what to do if they become victims of cybercrime. Since so much of our financial lives happen online, having a simple cybersecurity plan can help you respond quickly and minimize potential damage.

Protect Your Most Important Accounts
Secure your online banking, email, payment apps, and other sensitive accounts by using strong, unique passwords and enabling multi-factor authentication (MFA) whenever it's available.

Know How to Respond
If you believe an account has been compromised:

- Change your password immediately.
- Contact your bank or service provider.
- Monitor your accounts for suspicious activity.
- Scan your device for malware if needed.

Acting quickly can help limit financial losses.

Make Cybersecurity a Family Priority
Talk with family members about recognizing phishing emails, avoiding suspicious links, and protecting personal information. Business owners should also encourage employees to report suspicious emails or unusual requests.

Stay Prepared
Cyber threats continue to evolve, but a few simple habits can make a big difference. By preparing now, you'll be better equipped to protect your personal information and financial accounts in the future.

If you ever have concerns about suspicious account activity, contact us right away. We're here to help you protect your financial well-being.

Source: OpenAI, ChatGPT, July 23, 2026

Are Your Browser Extensions Helping...or Hurting? What You Need to Know

Browser extensions can make everyday tasks easier. They can block ads, save passwords, check grammar, compare prices, or help manage your schedule. While many extensions are legitimate and useful, others can put your personal and financial information at risk.

Cybercriminals have increasingly used malicious or poorly secured browser extensions to collect browsing activity, steal login credentials, or redirect users to fraudulent websites. Understanding the risks can help you make safer choices while browsing the internet.

What Is a Browser Extension?
A browser extension is a small software program that adds features or functionality to your web browser, such as Google Chrome, Microsoft Edge, Firefox, or Safari. Many are free to download and install with just a few clicks.

However, some extensions request extensive permissions that allow them to view websites you visit, read information you enter into online forms, or access saved passwords.

Warning Signs of a Risky Extension
Before installing a browser extension, consider the following:

- Does it come from a reputable developer?
- Does it have a large number of legitimate user reviews?
- Has it been updated recently?
- Does it request permissions that seem unnecessary for its purpose?

For example, a coupon-finding extension probably doesn't need access to your online banking activity or email accounts.

Best Practices for Staying Safe
To reduce your risk:

- Install extensions only from your browser's official extension store.
- Read the permissions carefully before clicking "Install."
- Remove extensions you no longer use.
- Keep your browser and extensions updated.
- Periodically review the extensions installed on your devices.

Remember, fewer extensions generally mean fewer potential security risks.

Tips for Business Users
Browser extensions can also present risks in the workplace. Employees who install unauthorized extensions on company devices may unintentionally expose sensitive business information or customer data. Businesses should consider establishing policies regarding approved browser extensions and regularly reviewing software installed on company computers.

Small Changes Can Make a Big Difference
Cybersecurity often comes down to the small decisions we make every day. Taking a few minutes to review the browser extensions installed on your computer can help reduce your exposure to fraud, identity theft, and malware.

As your community bank, we're committed to helping you protect your financial information both online and offline. If you have questions about safe online banking practices or notice suspicious account activity, please contact us. Together, we can help keep your financial information secure.

Source: OpenAI, ChatGPT, July 23, 2026

Image by: magnific.com