Bank of Botetourt

December 2025

2025 Year in Review: The Top Cyber Scams of the Year

As we close out 2025, one trend is unmistakable: cybercriminals have become more sophisticated, more organized, and more convincing than ever before. Both individuals and small businesses were targeted at a record pace, with scams growing more believable and harder to detect.

Bank of Botetourt remains committed to helping you stay informed, protected, and confident when it comes to your financial security. Below is a deeper look at the top cyber scams we saw this year—what they looked like, how they worked, and how you can protect yourself going forward.

1. AI-Powered Impersonation Scams
Artificial intelligence has enabled scammers to mimic voices, writing styles, mannerisms, and even live video feeds. These schemes were especially dangerous because they targeted both emotions and urgency.

How the scam works

- ✓ Voice cloning: Scammers use AI to duplicate the voice of a CEO, spouse, adult child, or friend. Victims receive urgent calls requesting money transfers or sensitive information.
- ✓ Deepfake video calls: Criminals impersonate company executives in video meetings to authorize fraudulent payments.
- ✓ Email "style" cloning: AI analyzes public writing samples (emails, social posts) to generate messages that read exactly like the person being impersonated.

Real-world example
A small business employee received an urgent video call that appeared to be from their CFO, instructing them to pay a vendor immediately using updated wire instructions. The "CFO" was an AI deepfake. The business lost $47,000.

How to protect yourself

- Always verify unexpected requests involving money or personal information using a known phone number, not the one provided in the message.
- Establish a bank-approved secure process for confirming wires and transfers.
- Encourage family members—especially teens and older adults—to create a family verification phrase used only in emergencies.

2. Package Delivery & QR Code Scams
With online shopping more popular than ever, scammers have shifted tactics to exploit delivery notifications and QR codes.

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

How the scam works

- ✓ Victims receive texts or door tags stating that a package "requires redelivery fee" or "failed to deliver due to missing info."
- ✓ Messages contain a QR code or link directing victims to a fake shipping website.
- ✓ Logging in or entering payment information gives scammers access to accounts.

Why it's effective

The messages appear at the exact moment people are expecting multiple packages—during holidays, birthdays, and other peak shopping seasons.

How to protect yourself

- Avoid scanning QR codes from unsolicited messages or physical tags left at your door.
- Go directly to the official website of UPS, USPS, FedEx, or Amazon to check your delivery status.

3. Small-Business Invoice & Vendor Fraud

This was one of the most financially damaging scams of 2025 for business customers.

How the scam works

- ✓ Criminals intercept email conversations between a business and its vendors.
- ✓ They send legitimate-looking invoices that include a new bank account number.
- ✓ Payments are sent to the fraudulent account, often overseas, and are difficult to recover.

Tactics used

- Spoofed email addresses that differ by one character.
- Hijacked email threads from real vendor accounts that were previously compromised.
- Fake "updated bank instructions" with official-looking attachments.

How to protect your business

- Require dual approval for all payments.
- Implement a call-back verification protocol for invoice changes.
- Encourage employees to carefully inspect email addresses for subtle variations.

4. Subscription Renewal & Tech Support Scams

Pop-up notifications and emails claiming that your computer protection, streaming service, or software license was about to expire saw a sharp rise this year.

How the scam works

- ✓ You receive a notice stating you've been charged hundreds of dollars for a subscription renewal.
- ✓ A phone number is provided to "reverse the charge."
- ✓ When you call, scammers request remote computer access or personal banking details.
- ✓ They may walk you through "fixes" that actually compromise your device.

Why it works

These scams create a sudden shock ("I didn't authorize this!"), prompting quick action.

How to stay protected

- Never call numbers that appear in pop-ups.
- Close the window and check your subscription status by logging in directly to the provider's website.
- Use antivirus software from trusted brands only.

5. Cryptocurrency Investment Schemes

Crypto scams thrived again in 2025, but with more sophistication. Scammers promised extraordinary returns through AI trading platforms or exclusive investment programs.

How the scam works

- ✓ Victims are shown a professional-looking dashboard with fake profit data.
- ✓ Early withdrawals are sometimes honored with small payouts to build trust.
- ✓ Once larger sums are deposited, the platform disappears.

Trends we saw

- Scammers impersonated financial advisors on social media.
- Fraudsters "pig-butchering" victims—slowly building relationships before pitching fraudulent investments.
- Fake endorsements from celebrities and financial experts.

How to protect yourself

- Avoid any investment opportunity promising "guaranteed" returns.
- Consult a financial professional before sending money.
- Remember: legitimate banks, including ours, do not use Telegram, WhatsApp, or social media for investment outreach.

6. Social Media Marketplace Fraud

As more customers turn to platforms like Facebook Marketplace, Craigslist, and resale apps, scammers have followed.

How the scam works

For buyers:

- ✓ "Too good to be true" listings for electronics, vehicles, pets, or tickets.
- ✓ Seller requests a deposit or asks you to pay shipping before sending the item.

For sellers:

- ✓ Buyers send fraudulent cashier's checks or "overpay" by accident, asking for the difference back.
- ✓ Fake payment confirmation screenshots are used to trick sellers into shipping items before money is received.

How to avoid marketplace scams

- Meet locally in public places when possible.
- Do not send deposits for items you have not inspected.
- Use secure payment methods recommended by the platform.

We're Here Whenever You Need Us

If you ever receive a suspicious call, message, or email—or if something simply feels "off"—contact us before taking any action. We are here to help keep your financial information safe. Thank you for allowing us to serve you in 2025.

Source: Article: OpenAI, ChatGPT, November 21, 2025 https://chatgpt.com/

Cheers to 2026! A Festive Guide to Staying Cyber-Safe in the New Year

As we ring in 2026 with glittering countdowns, fresh goals, and maybe a few leftover holiday cookies, it's also the perfect time to give your digital life a little seasonal tune-up. Cybercriminals don't take holidays—but that doesn't mean staying secure has to be stressful.

To start the year on a merry and confident note, here are some fun and festive cybersecurity tips to carry with you into 2026.

1. Unwrap New Devices Carefully
Did you receive a new phone, laptop, tablet, or smart home gadget? Before you dive in:

- ✓ Install updates (think of them as the "batteries included" part of adulting).
- ✓ Change default passwords—"admin" and "1234" are the cyber equivalent of leaving your front door wide open.
- ✓ Enable multi-factor authentication so only you have the key.

Your new tech will thank you!

2. Start the Year With a Password Makeover
New year, new… passwords? We know it doesn't sound glamorous, but it is one of the best ways to protect yourself.

Try this festive routine:

- ✓ Turn old passwords into long passphrases (e.g., "SnowflakesOnMainStreet2026").
- ✓ Use a password manager to make life easier.
- ✓ Retire that one password you use everywhere—we all have one, and yes, this is the year to let it go.

3. Cozy Up and Review Your Accounts
On a quiet winter morning, grab a warm drink and take a quick peek at your financial accounts. Look for anything unfamiliar or unexpected.

Just a five-minute review each month can help you spot trouble early—and your future self will thank you.

4. Beware of "Too Good to Be True" Holiday Deals That Last a Bit Too Long
If you see a "limited-time holiday sale" still going strong deep into January, it might be a scammer trying to lure you into clicking a link or sharing your card information.

When in doubt, go directly to the retailer's official website instead of clicking on mysterious "exclusive offers."

5. Brighten Your Business's Security with a Fresh Start
If you're a business owner, the new year is a perfect moment to refresh your internal security habits:

- ✓ Review who has access to accounts or payment systems.
- ✓ Update vendor contacts and confirm payment instructions.
- ✓ Remind your team how to spot suspicious emails—especially those with surprise "urgent" requests.

A little early-year housekeeping can prevent big headaches later.

6. Watch Out for Winter-Blues Scams
January is prime time for fake "budgeting apps," resolution-themed subscription scams, and phony tech-support pop-ups claiming to "clean your device for the new year."

If an app or email promises to instantly fix your finances or your computer, it's worth a second look.

7. Celebrate by Backing Up Your Memories
Photos, documents, and holiday videos deserve protection too. Back them up to a secure cloud service or an external hard drive.

A fresh digital backup is a great way to start 2026 feeling organized and stress-free.

Here's to a Safe and Bright 2026!
Cybersecurity doesn't have to feel overwhelming—small steps throughout the year make a huge difference. And remember, Bank of Botetourt is always here to help. If you're ever unsure about a message, phone call, or transaction, reach out to us. We love being part of your financial peace of mind.

Wishing you a joyful, secure, and prosperous new year!

Sources/Credit:
Article: OpenAI, ChatGPT, November 21, 2025, https://chatgpt.com/
Image: Freepik; Freepik Terms of use

Designed by Freepik