Bank of Botetourt

June 2026

Vacation Season Cybersecurity: How to Protect Your Finances While Traveling

Summer travel season is a time to relax, recharge, and spend time with family and friends. However, while travelers are preparing for vacations, cybercriminals are preparing opportunities to target distracted consumers and businesses.

Whether you are traveling for leisure or business, taking a few cybersecurity precautions before and during your trip can help protect your financial information and reduce the risk of fraud.

Be Careful with Public Wi-Fi
Airports, hotels, coffee shops, and restaurants often provide free public Wi-Fi, but these networks may not be secure.

Cybercriminals can use unsecured networks to intercept sensitive information, including:

- Online banking logins
- Credit card information
- Email credentials
- Business data accessed remotely

Whenever possible:

- Avoid accessing financial accounts on public Wi-Fi
- Use your cellular network or a trusted hotspot instead
- Consider using a Virtual Private Network (VPN) for added protection

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

Continued on page 2

Protect Your Devices While Traveling
Smartphones, tablets, and laptops often contain significant personal and financial information.

Before traveling:

- Update device software and apps
- Enable strong passwords, fingerprint, or facial recognition
- Turn on device tracking and remote wipe features
- Back up important data

If a device is lost or stolen, these safeguards can help protect your information.

Watch for Travel-Related Scams
Summer travel also brings an increase in scam activity.

Be cautious of:

- Fake hotel or airline booking websites
- Fraudulent vacation rental listings
- "Too good to be true" travel deals
- Phishing emails claiming itinerary changes or payment issues

Always book travel through trusted providers and verify websites before entering payment information.

Tips for Business Travelers
Employees traveling with company devices or accessing business systems remotely should follow additional precautions:

- Use company-approved VPNs when accessing business systems
- Avoid using shared public computers
- Keep business devices with you whenever possible
- Report suspicious login attempts or device loss immediately

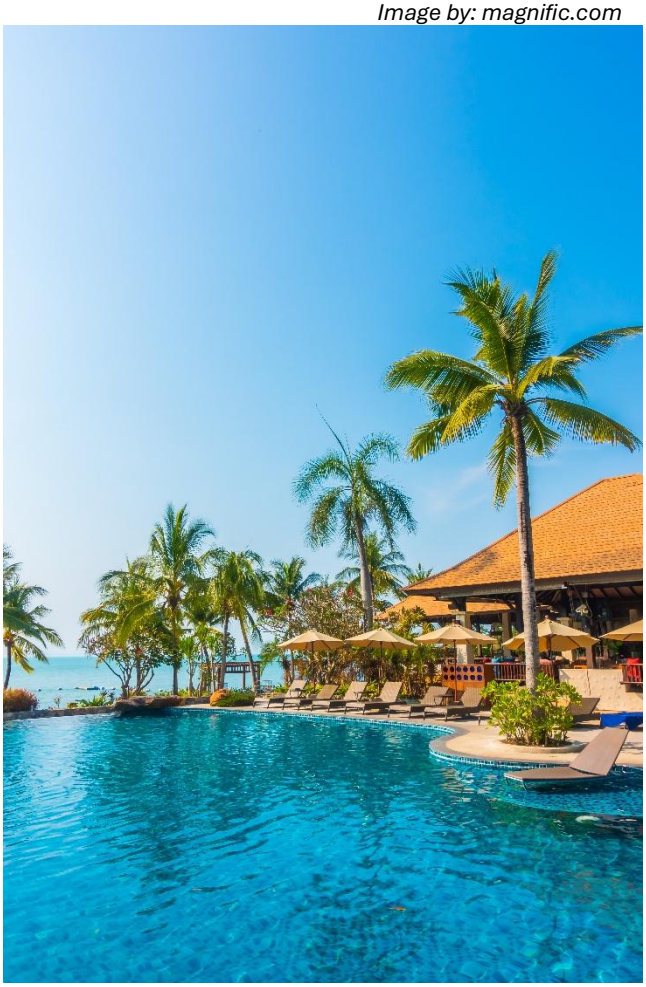
A compromised device can create risk not only for the individual traveler, but also for the organization.

Travel with Confidence
Cybersecurity awareness should travel with you wherever you go. A few proactive steps can help you enjoy your summer plans while keeping your financial information secure.

If you notice suspicious account activity while traveling, contact us immediately using a trusted phone number or official website. We are here to help protect your accounts wherever life takes you.

Source: OpenAI, ChatGPT, May 19, 2026

Image by: magnific.com



Password Security in 2026: Why Strong Passwords Still Matter

As technology evolves, so do the tactics used by cybercriminals. While security tools such as multi-factor authentication (MFA) continue to improve, passwords remain one of the most important lines of defense protecting personal and business accounts.

Weak or reused passwords continue to be a leading cause of account compromise, identity theft, and financial fraud.

Why Passwords Are Still Important
Cybercriminals use automated tools capable of testing thousands of password combinations in seconds. If a password is simple, predictable, or reused across multiple accounts, the risk increases significantly.

A compromised password can provide access to:

- Online banking platforms
- Email accounts
- Payment apps
- Business financial systems
- Stored personal information

Because many accounts are interconnected, one weak password can create broader exposure.

Best Practices for Strong Passwords
A secure password should be:

- Long and unique
- Difficult to guess
- Different for every account

Consider using:

- A passphrase instead of a single word
- A combination of letters, numbers, and symbols
- A password manager to securely store credentials

Avoid using:

- Birthdates or family names
- Common words or predictable sequences
- The same password across multiple accounts

The Importance of Multi-Factor Authentication
Even strong passwords benefit from additional protection.

Multi-factor authentication (MFA):

- Adds a second verification step
- Helps prevent unauthorized access if a password is stolen
- Is strongly recommended for banking, email, and business systems

Whenever available, enable MFA on your accounts.

Password Security for Businesses
Businesses should establish clear password and authentication policies for employees.

Recommended practices include:

- Requiring strong, unique passwords
- Enforcing regular security training
- Limiting access based on job responsibilities
- Implementing MFA across company systems

Employee awareness remains one of the most effective cybersecurity tools.

Small Habits Make a Big Difference
Cybersecurity does not always require complex technology. Often, consistent habits, such as using strong passwords and enabling MFA, provide meaningful protection against fraud and unauthorized access.

We are committed to helping our customers bank securely and confidently. If you have concerns about account security or suspicious activity, please contact us directly using a trusted phone number or official website.

Source: OpenAI, ChatGPT, May 19, 2026

Image by: magnific.com