The Evangeline BANK AND TRUST COMPANY

Secure Mobile Banking: Protecting Your Information on the Go

Mobile banking allows customers to manage accounts, transfer funds, deposit checks and monitor transactions anytime and anywhere. While these services offer convenience and flexibility, fraudsters increasingly target mobile devices to gain access to sensitive financial information.

The Evangeline Bank and Trust Company is committed to helping customers understand the risks associated with mobile banking and some steps they can take to protect their personal and financial information.

Understanding the Risks of Jailbroken and Rooted Devices

Smartphones and tablets include built-in security features designed to protect users from cyber threats. However, some individuals choose to "jailbreak" (Apple devices) or "root" (Android devices) to remove manufacturer restrictions and gain additional control over their devices.
While this may allow users to customize their devices or install unauthorized applications, it also removes important security protections.

Why Is This Risky?
When a device's security controls are disabled, cybercriminals may have an easier time:

- Installing malicious software without detection.
- Stealing usernames, passwords and banking credentials.
- Monitoring activity performed on the device.
- Gaining unauthorized access to personal and financial information.

Many financial applications rely on the device's built-in security controls to help protect account information. Removing these protections significantly increases the risk of fraud and identity theft.

Best Practices

- Keep your device's security protections enabled.
- Download applications only from official app stores.
- Avoid installing unauthorized or modified software.
- Use strong passwords and multifactor authentication whenever available.
- Monitor your financial accounts regularly for unusual activity.

Identifying Phishing Attempts Through Text Messages (SMS)

Cybercriminals frequently use text messages, commonly called "smishing" attacks, to trick consumers into revealing sensitive information.
These messages often appear to be from a bank, delivery service, government agency or other trusted organization.
Examples may include messages claiming:

- Your account has been locked.
- Suspicious activity has been detected.
- A package delivery requires payment.
- Immediate action is needed to avoid account closure.

The message usually includes a link directing the recipient to a fraudulent website designed to steal login credentials and personal information.

Warning Signs of a Smishing Attack
Be cautious if a text message:

- Creates a sense of urgency or panic.
- Requests passwords, PINs or verification codes.
- Contains misspelled words or unusual grammar.
- Includes suspicious links.
- Requests immediate action.

How to Protect Yourself

- Do not click links contained in unexpected text messages.
- Never provide account credentials or one-time security codes.
- Contact the organization directly using a trusted phone number if you have concerns.
- Delete and report suspicious messages.

The Evangeline Bank and Trust Company will never contact customers by text message and ask for passwords, PINs, account numbers or security codes.

Why Mobile Updates Matter

Many cyberattacks exploit known software vulnerabilities that have already been fixed by device manufacturers. Mobile operating system and application updates contain critical security patches designed to protect against newly discovered threats.
Ignoring updates can leave your device vulnerable to malware, fraud and unauthorized access.

Benefits of Keeping Devices Updated
Regular updates help:

- Fix security vulnerabilities.
- Improve device stability and performance.
- Protect against newly identified cyber threats.
- Enhance compatibility with banking applications.
- Strengthen security protections.

Best Practices

- Enable automatic updates whenever possible.
- Install operating system updates promptly.
- Update mobile banking applications regularly.
- Remove applications that are no longer used.

Keeping software up to date is one of the simplest and most effective ways to protect your information.

Risks of Using Unsecured Public Wireless Networks

Free Wi-Fi is commonly available at hotels, restaurants, coffee shops, airports and other public locations. While convenient, public networks may expose users to additional security risks.
Cybercriminals often target public wireless networks because they know people may use them to access sensitive information.

Common Public Wi-Fi Threats
Fake Wireless Networks
Criminals may create wireless networks that appear legitimate. Once users connect, attackers can collect information entered on the device.
Network Monitoring
On some unsecured networks, bad actors may attempt to monitor internet traffic to gather valuable information.
Fraudulent Login Pages

Attackers may present fake login screens designed to capture usernames and passwords.

Malware Distribution

Some unsecured networks may be used to spread malicious software to connected devices.

Protecting Yourself on Public Wi-Fi

- Avoid online banking activities while connected to public Wi-Fi.
- Use your mobile carrier's data connection when handling sensitive information.
- Confirm the correct network name before connecting.
- Disable automatic Wi-Fi connections to unknown networks.
- Log out of accounts when finished.

When possible, wait until you are on a trusted network before accessing financial accounts.

Mobile Malware Protection and Mobile PIN Security

Mobile malware is malicious software designed to infect smartphones and tablets. Criminals use malware to steal information, monitor activity and gain unauthorized access to accounts.

Mobile malware is commonly delivered through:

- Fake applications.
- Malicious links in emails and text messages.
- Infected websites.
- Unauthorized software downloads.

Ways to Protect Against Mobile Malware

- Download apps only from official app stores.
- Review app permissions before installing.
- Avoid clicking suspicious links.
- Keep devices updated.
- Remove applications you no longer use.

Protecting Your Mobile PIN

Your mobile PIN helps secure access to your device and mobile banking applications.

Best Practices for PIN Security

- Use unique PINs that are difficult to guess.
- Avoid using birthdays, addresses or repeated numbers.
- Never share your PIN with anyone.
- Do not write your PIN where it can be easily found.
- Enable biometric authentication when available.

Strong PIN security provides another layer of protection if a device is lost or stolen.

Auto-Wipe Features and Application Password Protection

Many mobile devices include security features designed to protect data if the device is lost, stolen or compromised.

What Is Auto-Wipe?

Auto-wipe features automatically erase sensitive information after multiple failed login attempts or allow users to remotely erase a lost device.

This helps prevent unauthorized individuals from accessing personal or financial information.

Benefits of Auto-Wipe Features

- Protects sensitive information from unauthorized access.
- Reduces the risk of identity theft.
- Helps safeguard financial data stored on mobile devices.
- Protects user’s privacy.

Application Password Protection

Many mobile applications allow users to create app-specific passwords or require authentication each time the application is opened.
Using application passwords provides an additional layer of security beyond the device password.

Best Practices

- Enable passwords or biometric authentication for banking applications.
- Log out of banking applications when not in use.
- Use unique passwords for each application.
- Avoid storing passwords in unsecured locations.
- Enable multifactor authentication whenever available.