

Customer Information & Cyber Security Awareness

Rev. 2025-9

At **AmeriFirst Bank**, we take the safeguarding of information seriously. Keeping data safe and secure is every employee's responsibility. We also encourage you to take steps to protect your own personal information.

No employee of AmeriFirst Bank will ever email, text, or call you requesting personal information—including account numbers, passwords, driver's license numbers, or Social Security Numbers—by phone, email, or website link.

If you need to contact AmeriFirst Bank by email, **do not send privileged or personal information** through regular email, as it is not encrypted and therefore not secure. If you must send confidential information, contact a bank employee for a link to our **secure email portal**.

Protecting yourself from **scams, identity theft, malware, and ransomware** is more important than ever. Below are best practices to help safeguard your personal and financial information.

Best Practices for Cyber Safety

- **Change your passwords regularly** (at least every six months).
 - **Use unique passwords** for different accounts.
 - **Create strong passwords** with a mix of letters, numbers, and special characters.
 - **Enable multi-factor authentication (MFA)** wherever possible.
 - **Never share your password** with anyone.
 - **Do not store login information** where others can access it.
 - **Avoid public computers or public Wi-Fi** for online banking or sensitive transactions.
 - **Businesses** using online banking should **perform periodic risk assessments** and evaluate internal controls.
 - **Do not email confidential information** unless it is encrypted.
 - **Shred sensitive documents** such as bank statements, expired cards, and medical or insurance forms.
 - **Review account statements monthly** and report unauthorized charges immediately.
 - **Wipe data from old devices** (smartphones, tablets, computers) before disposal.
 - **Install apps only from trusted sources.**
 - **Keep your devices updated** with the latest operating system and security patches.
 - **Enable encryption and auto-lock** on mobile devices.
 - **Report suspicious emails** to the bank's IT or Security Department.
-

Phishing Awareness

Phishing is a scam where criminals attempt to trick you into revealing personal information through fake emails, texts, or phone calls. These messages often look legitimate, using company logos and familiar wording.

Key Tips:

- No reputable business will ever ask you to update account information, passwords, or Social Security Numbers via a link or email.
- **Never click links or call numbers** provided in suspicious messages. Open a new browser window and manually type the organization's web address or call a verified number.
- **Hover over links** to view the true website before clicking.
- **Report suspicious messages** to the bank or FTC.

Emerging Threat:

Criminals are using **AI-generated voice calls or messages** that sound real. Always verify unexpected or urgent requests before taking action.

Ransomware & Malware

Ransomware is malicious software that locks or encrypts your files and demands payment—often in cryptocurrency—to restore access.

Common Attack Methods:

- Fake phone calls claiming to be from reputable companies (Microsoft, Norton, etc.).
- Phishing emails prompting you to click a link or download an attachment.
- Pop-up messages from infected websites.

Protection Tips:

- Keep **operating systems and software** fully updated.
 - Use **up-to-date antivirus protection** on all devices.
 - **Backup your files** regularly on a separate device or secure cloud service.
 - **Do not open emails or attachments** from unknown senders.
 - **Be cautious on social media**—avoid clicking suspicious ads or links.
 - Verify any **security watermark or image** your financial institution uses before logging in.
 - **Report phishing or ransomware attempts** to your bank and the FTC.
-

Helpful Resources

- **Federal Trade Commission (FTC):** www.ftc.gov
 - **Homeland Security / OnGuard Online:** www.onguardonline.gov
 - **Identity Theft Help:** www.identitytheft.gov
-

If You Notice Suspicious Activity

Contact **AmeriFirst Bank** immediately at **1-800-298-1763** or any branch:

- Union Springs: 334-738-2060
- Vaughn Road: 334-409-2980
- Prattville: 334-358-0351
- Lee County: 334-821-1329
- Escambia County: 251-296-5356