Information Security Basics

AmeriFirst Bank | Rev. 2026-10

Protect your information with a few everyday habits: secure your accounts, check unexpected requests, keep devices updated, and report problems promptly.

Email, texts, and phishing

Verify before you act. Only open attachments or follow links when you have checked that the message and request are legitimate. A familiar sender or existing email conversation can be compromised. Contact the person or organization through a separate, trusted channel when a request is unusual.

Use a known route. Open the official app, use a saved bookmark, or type the organization's known website address yourself. Do not use a phone number supplied in a suspicious message. Treat unexpected QR codes like unfamiliar links.

Watch for pressure. Threats of account closure, urgent payment demands, unexpected refunds, and requests for passwords or verification codes are warning signs. Logos, polished writing, and correct personal details do not prove a message is genuine.

Handle suspicious messages safely. Do not reply or use their "unsubscribe" links. Use your email service's report-phishing or junk option. At work, follow your employer's reporting procedure. Do not forward suspicious attachments unless your security team instructs you to do so.

Be careful with all file types. Unexpected archives, executable files, documents, and PDFs can be harmful. Do not enable macros or bypass security warnings to view a document. Never send confidential information through ordinary email; use an approved secure method.

Passwords and sign-in protection

Choose long, unique passwords. Aim for 15 or more characters where supported, or use a long passphrase. Avoid predictable phrases and personal details. Follow the service's requirements and use a different password for each account. Change a password promptly if it is exposed or suspected stolen, including when it was reused on a compromised service.

Store passwords securely. A reputable password manager, including a properly secured built-in manager, can generate and save unique passwords. Protect the device and password-manager account with strong sign-in protection. Never save passwords on shared or public devices. For work accounts, use only employer-approved tools and follow workplace policy.

Turn on multi-factor authentication (MFA). Where available, use a passkey or security key for phishing-resistant sign-in. An authenticator app is another option. Do not disclose passwords, PINs, or verification codes to someone who contacts you, and deny sign-in prompts you did not initiate. Keep recovery details current and store backup recovery codes securely.

Everyday Security & Scam Awareness

Devices, browsing, and Wi-Fi

Install operating system, browser, app, and security updates promptly. Use supported security software where appropriate. Download apps from trusted sources, review permissions, and enable automatic screen locks and device encryption.

Avoid public or shared computers for banking. On any network, use the official app or check the full website address and HTTPS connection. **HTTPS encrypts the connection; it does not prove a site is legitimate.** Never ignore certificate warnings. A VPN does not make a phishing website safe.

Do not call numbers shown in unexpected security pop-ups or install remote-access software at a stranger's direction. Use your own charging adapter and cable or a power bank when possible; decline unexpected requests to trust a computer or share device data.

Social media, documents, and backups

Limit public personal details, travel plans, and information that could help someone impersonate you. Review privacy settings and app access. Keep work and personal accounts separate and follow your employer's rules for business email and social media.

Lock devices when unattended. Store sensitive papers securely and shred them before disposal. Securely erase devices before selling, recycling, or discarding them. Keep protected backups separate from working files, such as a disconnected external drive or cloud backup with recovery history, and test that files can be restored.

Calls, payment requests, and impersonation

Caller ID, voices, and videos can be faked, including with AI. Verify unexpected family, employer, bank, or government requests by calling a number you already know is correct. Before changing vendor or payroll payment instructions, verify independently and obtain any required second approval.

Never move money to a supposed "safe account" because of an unexpected call or message. Demands to pay a tax, fine, fee, or account problem with gift card numbers are scams. Be suspicious of pressure to send cryptocurrency, withdraw cash for collection, or keep a transaction secret. Stop and verify independently.

If information, an account, or money is at risk

For banking concerns, contact **AmeriFirst Bank at 1-800-298-1763** immediately. Tell us if you shared credentials, approved an unfamiliar sign-in, sent money, or noticed an unauthorized transaction. Ask whether a payment can be stopped or recovered; recovery is not guaranteed. For a workplace incident, notify your employer's IT or security contact promptly.

Use a trusted device to secure affected accounts through the provider's official recovery process. Change compromised passwords, sign out other sessions, and review recovery settings. If you suspect malware, disconnect the affected device from networks and get trusted technical help before banking on it again. Keep messages and transaction records.

Type these addresses into your browser: amerifirstbank.com (bank website); **my.amerifirstbank.com** (online banking); **ReportFraud.ftc.gov** (scam reporting); **IdentityTheft.gov** (identity theft recovery); **IC3.gov** (internet crime reporting).