Compromised Email Account

AmeriFirst Bank | Rev. 2026-11

Your email can be used to reset passwords for banking, shopping, and other accounts. If you suspect someone has access, act quickly to secure it and check for related fraud.

Recognize the warning signs

You cannot sign in; you receive unexpected password or recovery changes; your contacts receive messages you did not send; or you see unfamiliar sign-ins, missing messages, or changes to mailbox settings.

A forged sender address can also make a message look as if it came from you. An unexpected message alone does not prove someone accessed your account, but it is a reason to check your security settings.

Take back control

1. Use a trusted device and your provider's official recovery process

Go directly to your email provider's official website or app. Do not use links or phone numbers in suspicious messages or ads offering account recovery. If you cannot sign in, use the provider's account recovery option. For work or school email, contact your IT support team promptly.

2. Change your password and end other sessions

Create a long, unique password or passphrase you have not used elsewhere. Use the provider's option to sign out other devices and sessions. Changing a password may not end every session or remove all app access, so complete the remaining checks.

3. Check recovery information and account access

Review your recovery email, phone number, security questions, trusted devices, and sign-in methods. Remove unfamiliar entries. Review connected apps, delegated access, and app passwords; revoke access you do not recognize. Follow your provider's instructions if you cannot remove a change.

4. Review mailbox rules and forwarding

Remove unauthorized forwarding addresses, inbox rules, filters, and automatic replies. Check your signature and Sent, Deleted, and Trash folders for unexpected changes or messages.

Protect Your Other Accounts

5. Strengthen sign-in protection

Turn on multi-factor authentication (MFA). Use a passkey, security key, or authenticator app when supported. Remove unfamiliar MFA methods and regenerate backup codes if they may have been exposed. Never share a security code or approve a sign-in you did not initiate.

6. Check linked accounts and warn your contacts

After securing your email, review banking, payment, shopping, and social media accounts for unusual activity. Change any reused or exposed passwords. Tell contacts through a trusted channel to ignore unexpected links, attachments, payment requests, or bank-detail changes sent from your account.

7. Check your devices

Install operating system, browser, and app updates. Run a scan using trusted, updated security software. If you suspect a device is infected, use another trusted device to secure your accounts and get help cleaning the affected device before using it again.

If your money or personal information may be affected

Contact AmeriFirst Bank immediately if you see unfamiliar transactions, exposed banking credentials, or messages changing payment instructions. Use a known bank number or the number on the back of your card. Do not use contact information supplied in a suspicious message.

Review activity through the bank's mobile app or type **my.amerifirstbank.com** into your browser. The bank's website is **amerifirstbank.com**. Do not email account numbers, passwords, Social Security numbers, or other sensitive information through regular email.

AmeriFirst Bank: 1-800-298-1763

If identity theft is suspected, type **IdentityTheft.gov** into your browser for a recovery plan. Report scams at **ReportFraud.ftc.gov**. Save relevant messages, screenshots, and transaction details.

Reduce the chance of another compromise

Use a different password for every account and consider a reputable password manager. Keep recovery details current, enable sign-in alerts when available, and review account activity. Use your own trusted device for sensitive accounts. Verify unusual requests through a separate, trusted contact method before sending money or sharing information.

Sources and additional guidance

Federal Trade Commission - Recover a hacked account
consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account

Microsoft Support - Search for "How to recover a hacked or compromised Microsoft account"
support.microsoft.com

Type these addresses into your browser to access the guidance.