Five steps to avoid phishing scams

Phishing scams can come from fraudsters via text, email, or a phone call and often use an urgent tone to push you to act quickly.

They may pose as someone you know or as a legitimate organization to ask for an immediate payment or sensitive information.

Remember that you should **never share** your PIN, online banking password, account number or personal information, and one-time access codes with anyone. AmeriFirst Bank will **never call you and ask** for this information.

Here are five steps to help spot, avoid, and report phishing attempts.

Step 1: Be alert. Know the phishing warning signs.

Phishing messages can skillfully imitate your bank, a government agency, or another organization you recognize or trust.

Beware of email addresses that do not include "amerifirstbank.com."

1. **Use caution with urgent alerts** that ask you to act immediately.
2. **Avoid clicking on links or calling numbers** you don't recognize.

When in doubt, sign on to AmeriFirst Bank website (www.amerifirstbank.com) or contact us directly by calling the number on the back of your card.

Step 2: Pause. Go slow when you spot false urgency.

Phishing attempts often arrive as an urgent request.

Be suspicious of messages that announce a "problem" with your account or ask you to immediately log in to unlock your account, verify a transaction, make an online payment, or reverse a payment.

When asked to "act immediately," do the opposite. Go slow and resist the urge to respond right away.

Step 3: Verify. Confirm the sender but don't rely on caller ID.

Phishing attempts can be sophisticated and may even spoof (or imitate) caller ID making the call look legitimate.

Don't assume a communication can be trusted simply because it appears or sounds legitimate.

Contact the organization directly by going to their website.

To verify communications that appear to be from AmeriFirst Bank, sign on using the Mobile APP or type "amerifirstbank.com" into a new browser tab to access AmeriFirst Bank online banking directly.

Step 4: Stop. When in doubt, don't respond.

When you receive an urgent request that doesn't seem right, hang up or close the message. You aren't being rude — you are being wise.

Actions to avoid:

- Do not sign on to your account from a link embedded in a suspicious message
- Do not share personal account information such as your PIN, password, account number or one-time access codes
- Do not click any links or open attachments, which can install malware on your device
- Do not call phone numbers included in the communication
- Do not allow remote access to your computer

Step 5: Let us help. Report phishing if it happens.

Be sure to use Online Banking to regularly monitor your account for suspicious activity. You can also turn on additional alerts to be notified of transactions and withdrawals.

If you've fallen victim to phishing

Call us immediately at **1-800-298-1763** if you clicked a link, opened an attachment, sent a payment, or provided personal or financial information in response to a suspicious message.

If you've spotted a phishing attempt

If you see a suspicious message mentioning AmeriFirst Bank, but didn't click on the link or open any attachments, forward the message to us at **customerservice@amerifirstbank.com** and then delete it.

If the suspicious message is unrelated to AmeriFirst Bank, consider contacting that organization directly to report the incident.

When to report fraud

If you suspect you were the victim of fraud related to your account, contact your local office or at 1-800-298-1763us immediately.