STAY SECURE WHEN USING AI TOOLS

Think Before You Share. Verify Before You Act.

AI tools can help your business save time and work efficiently, but information entered into them may be stored or used by the provider. Protect your business by following these tips:

- **Keep Sensitive Information Private** - Never enter banking credentials, account or card numbers, one-time passcodes, customer data, or confidential business information.
- **Use Approved Tools** - Follow your company's security and privacy policies when it comes to AI, and only use approved tools for business use.
- **Verify Before Acting** - Confirm payment requests, account changes, invoices, and wire instructions by calling a known, previously verified phone number, not a number provided in the request.
- **Verify AI-Generated Information** - Independently verify the accuracy and completeness of AI-generated information before relying on it to make financial, compliance, operational, or business decisions.
- **Watch For AI-Enabled Scams** - Be cautious of urgent or unusual emails, messages, voices, and images, even when they appear to come from someone you know.
- **Secure Your Access** - Use strong, unique passwords, enable multifactor authentication using a method other than email, and keep devices and applications updated.

If you believe your online banking information or accounts may have been exposed, stop the interaction and contact us promptly through a trusted channel.

Remember:

Use AI as a helpful resource—not as a substitute for verification, security controls, or good judgment.

Banterra®

866-BANTERRA | BANTERRA.BANK | MEMBER FDIC