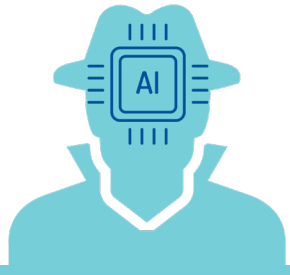
Don’t Be Spoofed

How AI Scams Are Targeting Bank Customers



In recent months, the banking industry has sounded alarms about a surge in spoofing (when a scammer mimics a trusted entity to deceive and steal) and impersonation scams powered by artificial intelligence (AI). Unlike the more obvious scams of decades past, these attacks now imitate the tone, language, and even real voices making them nearly indistinguishable from genuine communications.

Accessibility of generative AI tools has broadened fraudsters’ capabilities significantly. Hyper-personalized phishing emails crafted with AI emulate known contacts or institutions, making victims more likely to fall for them. These fraudsters exploit the lack of awareness among consumers and institutions alike and many still rely on authentication methods AI has recently deemed ineffective.

What Consumers Can Do to Stay Safe

1. Verify Communications

If you receive a call, text, email, or video claiming to be from your bank, stop and verify through trusted channels. Call your bank back using the number on your official statement or website. Be especially skeptical of urgent or emotionally charged messages that cause distress or require immediate action.

2. Use Strong Authentication Methods

Enable multi-factor authentication (MFA) wherever possible. This extra layer of security can stop scammers even if they know your password. Banks and regulators are urging the adoption of stronger verification systems, as voice-based and other common methods are no longer reliable due to AI’s sophistication.

3. Strengthen Your Digital Hygiene

Use unique, robust passwords or passphrases, and avoid sharing credentials or one-time codes with anyone. Keep your devices and apps updated to benefit from the latest security improvements.

4. Compare Legitimate Communications

Familiarize yourself with how your bank will and will not communicate. Save genuine, verified text messages or emails for reference. Be wary of highly polished messages. Fraudsters can now replicate styling, sender addresses, and even writing tone.

5. Learn How to Detect Advanced Scams

This infographic from the American Bankers Association and FBI includes tips on spotting deepfake scams and recognizing AI impersonation: www.aba.com/news-research/analysis-guides/deepfake-media-scams.

As AI continues to blur the line between genuine and fraudulent communication, it’s more important than ever to stay vigilant. No single safeguard is foolproof, so layering personal caution with current technology protections is key. When in doubt, reach out directly to your bank. Your awareness is your best defense.