# Social Engineering

**AmeriFirst Bank | Customer & Business Security Education | Rev. 2026-10**

## What is social engineering?

Social engineering is the use of deception or pressure to persuade someone to share sensitive information, send money, provide access, or bypass a safeguard. It can happen through calls, texts, email, social media, websites, QR codes, mail, or in person.

Scammers may pretend to be your bank, a government agency, a family member, a coworker, a vendor, or technical support. They can use stolen personal details, compromised accounts, and AI-generated voices or videos to make their story convincing.

## Recognize the pressure - not just the appearance

**Urgency or fear:** "Your account will be closed," "Your money is at risk," or "Act now to avoid arrest."
**Secrecy:** "Do not tell the bank, your family, or your supervisor."
**Authority or familiarity:** "I am calling from your bank," or "Your boss needs this today."
**Rewards or emotional appeals:** An unexpected prize, investment promise, refund, romance, or family emergency.
**Bypassing safeguards:** Instructions to ignore a warning, skip approval, share a code, or install software.

**Correct details do not prove identity.** A message can use your real name, account details, a familiar logo, or an existing conversation and still be fraudulent. Good grammar is not proof of legitimacy. Caller ID and voices can be faked. A padlock or HTTPS encrypts a connection but does not prove a website is genuine.

## Common examples

**Bank impersonation.** A caller claims a charge is fraudulent and asks you to read back a sign-in code, approve a login, or move money to a "safe account." Stop and call the bank independently.

**Fake technical support.** A pop-up or unexpected contact claims your device is infected and asks you to call a number, share your screen, or install remote-access software. Do not use the supplied contact details or grant access.

**Changed payment instructions.** A vendor or executive appears to request a new bank account, urgent wire, payroll change, or gift cards. A real email account may have been compromised. Verify through a known number before acting.

**Fake deliveries, refunds, and QR codes.** A message or package asks you to scan a code, pay a small fee, or sign in to resolve a problem. Check through the organization's official app or known website.

**Impersonated family or friends.** A convincing voice or message claims someone needs emergency money. Call that person or another trusted family member at a known number. Consider a family verification phrase.

# Pause. Verify. Protect.

## 1. Stop the interaction and check independently

You do not need to decide while someone is pressuring you. End the call or conversation. Open the official app, use a saved bookmark, or type the known website address yourself. Call a number from your statement, card, or existing records. Do not use a number or link supplied with the suspicious request.

## 2. Protect account access and confidential information

Never give passwords, PINs, or sign-in verification codes to someone who contacts you. Deny sign-in prompts you did not initiate. Do not send confidential information through ordinary email. When you initiate contact through a verified bank channel, the bank may need information to identify you or handle your request; verify the channel before sharing it.

Use long, unique passwords and multi-factor authentication (MFA). Where available, passkeys or security keys offer phishing-resistant sign-in. Keep recovery details current and limit personal information shared publicly. These safeguards help, but you still need to verify unusual requests.

## 3. Keep control of your money and devices

**Do not transfer money to a supposed "safe account" because of an unexpected call or message.** Requests to pay a tax, fee, fine, or account problem with gift card numbers are scams. Stop if someone pressures you to buy cryptocurrency, withdraw cash for collection, install remote-access software, or keep a transaction secret.

At work, follow visitor and access procedures. Do not let an unverified person into restricted areas or hand over equipment or records. Confirm technical-support requests through your organization's approved channel.

## 4. For businesses: verify payment changes

Confirm new or changed vendor, payroll, ACH, and wire instructions by calling an independently verified number. Do not rely only on an email reply or a number listed on the changed invoice. Use separate initiation and approval where available, and require a second authorized person to approve payment changes. Report suspicious requests to your own IT or security contact.

## 5. If you shared information, granted access, or sent money

**Contact AmeriFirst Bank immediately at 1-800-298-1763** if money or banking access is at risk. Explain what happened and ask whether affected access can be secured or a payment stopped or recovered. Recovery is not guaranteed. Do not wait for the suspected scammer to respond.

From a trusted device, use the account provider's official recovery process to change exposed passwords, sign out other sessions, and review security settings. If you granted remote access or installed software, stop using that device for banking and obtain trusted technical help. Keep messages, receipts, and transaction details. Beware of follow-up offers to recover your money for a fee.

## Trusted addresses - type them into your browser

**amerifirstbank.com** (bank website) | **my.amerifirstbank.com** (online banking)
**ReportFraud.ftc.gov** (scams) | **IdentityTheft.gov** (identity theft recovery)
**IC3.gov** (FBI internet-crime reporting)

Filing an online fraud report does not notify the bank. Contact the bank first when money or banking access is at risk.