MODULE 03: AI-GENERATED IMPERSONATION

The voice is real. The *person* is not.

A 45 minute session on calls and videos built from a real person's cloned voice or face. Three seconds of audio, taken from a voicemail greeting or a public video, is now enough to make a stranger's computer say anything in a voice the listener has trusted for decades. Written to be taught by a volunteer with no technical background.

VOICEMAIL, 2:47 PM

SPECIMEN, TEACHING MATERIAL ONLY

FROM: UNKNOWN CALLER

"Grandma, it's me. I'm okay, but I got into an accident and I — I'm at the police station, they said I can make one call. Please don't tell mom, she'll kill me. I need bail money, it's $3,200, my friend Steve is going to call you right after this with instructions. Please, I'm scared, just don't hang up on him."

NINETY SECONDS LATER. FROM: (312) 555 0191

"Hi, this is Steve, a friend of your grandson's. He's really shaken up. The court needs the bail processed through a bonds office, they only take it by wire or gift card today. I can walk you through it right now while it's still business hours."

The voice on the first call was real. It was assembled from clips of a real person talking, most likely pulled from a video he posted himself. Nothing about the call was faked in the sense of being computer generated from nothing. What was faked was who was speaking. The second call is the entire operation: a stranger, moving quickly, before anyone has time to call the grandson directly and find out he is at work.

The fixed structure

Every module in this series answers four questions in the same order: how the scheme works, the specific signals that separate it from a real emergency, the single action to take, and where to report it. This module follows that structure for calls and videos built from a cloned voice or face.

The point of the session

Most fraud prevention advice about phone scams assumes the listener can use their judgment about whether a voice sounds right. That assumption has quietly stopped being safe. A cloned voice does not sound almost right. It sounds like the person, because the software is not impersonating a voice from memory the way a human con artist would. It is reconstructing the actual acoustic pattern of that person's speech from a short recording, then generating new sentences in it. The participant's own certainty that they know their grandson's voice is now the thing being used against them, not their protection.

The session is not built to teach people to detect a fake voice by ear. Past a few seconds of generated audio, most people cannot, and audio quality keeps improving. It is built to teach one habit that works regardless of how good the fake is: verify through a channel the caller does not control, before doing anything the call asks for.

How the scheme works

The mechanics are consistent across the family emergency version, the romance scam video call, and the executive impersonation call to a business. All three follow the same three steps.

STEP	WHAT HAPPENS

Sourcing	A short clip of the real person's voice or face is collected. A voicemail greeting, a video posted publicly, a work meeting recording, or a voice message sent to anyone are all sufficient. Three to ten seconds of clean audio is typically enough for current cloning tools.
Generation	The collected sample is used to generate new speech, or in a video call, a live face and voice, saying whatever the caller wants said. Neither step currently requires technical skill. Both are available as consumer software.
Pressure	The generated voice or face is used to create urgency and demand secrecy in the same call, so the listener acts before verifying and does not mention it to anyone who could verify it for them.

The pressure step is where the scheme is most exposed, and it is why this module spends most of its time there rather than on the technology. The technology will keep changing. Urgency plus secrecy, in a request involving money, does not.

The specific signals

WHAT THE CALLER USES	WHAT IT IS ACTUALLY FOR
"Don't tell anyone"	Prevents the one thing that reliably breaks the scheme: the participant mentioning it to a family member who can confirm the real person is safe.
"I only have a minute"	Removes the time needed to think, look up a number, or call back.
A second caller joins	Moves the conversation to someone with a script, away from the emotional, harder-to-script cloned voice.
Payment by gift card, wire, or crypto	All three are effectively unrecoverable once sent. A legitimate court, hospital, or bail office does not ask for any of them.
Reluctance to do a live video call	Real-time video generation is harder to sustain convincingly than a short audio clip. A caller who avoids video, or whose video keeps “cutting out,” is avoiding the one channel most likely to expose the fake.

The single action

One habit defeats this scheme regardless of how convincing the voice or video is, because it does not depend on judging the voice at all.

1. Stay on the line, but stop talking about the emergency. Say only that you'll call them right back.
2. Hang up. Not out of rudeness. Ending the call ends the pressure.
3. Call the person back on the number already saved for them, not any number given during the call.
4. If they don't answer, call another family member who would know where they actually are.
5. Never send money, a gift card code, or a wire based on a call alone, however urgent it sounds or however certain the voice seemed.

THE FAMILY CODEWORD

Agree on a word or short phrase with close family in advance, to be used only if someone is asking for money or bail in a moment of real distress. A cloned voice can say anything the software is told to say, but it cannot know a word that was never spoken into a recording that was captured. Keep it simple, keep it private, and treat any emergency call that can't produce it as unverified until confirmed another way.

IF MONEY HAS ALREADY BEEN SENT

For a wire transfer, call the bank immediately and ask for the fraud department; recovery is possible in the first hours but the odds fall fast. For a gift card, call the number on the back of the card and report it as used fraudulently before the codes are redeemed. For cryptocurrency, treat it as gone; report it anyway, since reports feed the pattern that eventually leads to arrests. In every case, write down the phone number that called, the time, and exactly what was said, before the details fade.

Where to report

WHO	CONTACT	USE IT FOR
Federal Trade Commission	`reportfraud.ftc.gov` Online report, no phone needed	The first stop for any impersonation scam, whether or not money was lost. Builds the pattern data used to identify active scam networks.
FBI Internet Crime Complaint Center	`ic3.gov`	Required for any case involving a wire transfer, cryptocurrency, or losses over a few hundred dollars. Law enforcement uses IC3 reports to open investigations.
Your bank or wire service	Number on the back of your card, or on a statement	Immediately, if any transfer was made. Ask specifically for the fraud department, not general customer service.
AARP Fraud Watch Network Helpline	**877-908-3360** Free to anyone, member or not	Talking it through with a trained volunteer, including while a call is still active, or immediately after one has ended.
Local police	Non-emergency line	Filing a local report, which some banks require before reversing a transaction, and which documents the scam in your area.

DERIVED FROM

Operational scheme characterization developed alongside transaction and synthetic identity fraud detection work, and delivered through AARP's Fraud Fighter Network since May 2024.

REVISION

Version 1.0, published June 30, 2026. Revised as voice and video cloning tools change. Changelog: www.ayomideayeni.com

CORRECTIONS

Report an error, an out of date phone number, or a scheme variant this module does not cover: ayeniayomide5@gmail.com

> Ayeni, A. 2026. AI-generated impersonation (Module 03, Fraud prevention curriculum), version 1.0. Licensed CC BY 4.0.