

How to teach the one about *a voice you trust*

Everything a volunteer needs to deliver this module competently: what to do in the twenty minutes before, how to run each segment, what the exercise is actually testing, what to do when somebody says a version of this happened to them, and what never to do regardless of how much it would help.

THE SHAPE OF THIS SESSION

45 MINUTES • FOUR FIXED PARTS

0:00 to 0:12

PART 01

How the scheme works

Play or read the voicemail specimen.
Establish that the voice is real audio,
reassembled, not an actor.

0:12 to 0:19

PART 02

The specific signals

Secrecy, urgency, a second caller, gift
cards. Five signals, memorized as a set.

0:30 to 0:38

PART 03

The single action

Hang up, call back on a known number.
Set the codeword live, in the room.

0:38 to 0:45

PART 04

Where to report

Numbers on the handout, read aloud
once, not lingered on.

The exercise sits between parts 02 and 03, from 0:19 to 0:30. It is the longest single block in the session and the first thing a nervous facilitator cuts. Do not cut it. Everything before it is explanation, and explanation on its own has never set up a codeword with anybody's actual family.

COVERS Module 03 only Each module has its own guide	TEACH IT TO Anyone with a phone Effectively everyone. Especially useful for close-knit families.	PREPARATION 90 minutes, first time 20 minutes each delivery after
SESSION LENGTH 45 minutes 11 minute exercise included	THE MODULE www.ayomideayeni.com Read it before this guide	VERSION 1.0 Published June 30, 2026
LICENSE CC BY 4.0 Copy, adapt, and teach it	GOVERNING RULES Your host organisation's Where they differ from this, theirs win	

WHAT THIS GUIDE IS · Written so that the author is not required

Material that only works when its author is in the room is a service. Material a stranger can pick up and deliver well is something else. This guide exists to make the second thing true of Module 03.

The module is derived from work characterizing how voice and video cloning scams are actually built: what audio a scammer needs, how little of it, and what the resulting call is designed to make a listener do. That derivation gives the material its specificity. It does not, on its own, make the material teachable, which is a separate problem with a separate answer.

That answer is the fixed structure shown above. Every module in this series answers the same four questions in the same order, so a facilitator who has run one session knows where everything is in the next. The content is new each time. The floor under your feet is not.

Two things follow, and both are worth saying to anyone about to deliver this. You do not need to be able to explain how voice cloning software works. You need to run the shape and be honest about the edges of what you know. And the genuinely difficult part of this session is not technical, it is the thirty seconds after somebody says a version of this happened to their family, which is why that moment gets its own section below.

WHERE THIS GUIDE DOES NOT GOVERN

If you are delivering under the auspices of an organisation, that organisation's conduct rules, safeguarding policy, and escalation procedure take precedence over everything below. This guide assumes an independent community session with no such policy in place. Where one exists, follow it.

RUNNING IT WELL

Part 01, how the scheme works. Read the voicemail specimen aloud, slowly, in a flat voice, rather than performing it. The content does the emotional work; performing it on top of that reads as theatrical and undercuts the moment when you explain the voice was real audio. After reading it, say the single most important sentence in the module before anything else: the voice was not faked, the person was. That distinction is what the rest of the session rests on.

Part 02, the specific signals. Go through the five signals as a list, but spend real time on secrecy specifically. It is the signal that does the most work and the one participants are most likely to have already encountered in an unrelated context (a controlling relationship, a workplace instruction not to loop in HR) without recognizing it as a manipulation pattern. Naming it as a pattern, not just a fact about this scheme, tends to be the moment the room leans in.

The exercise, 0:19 to 0:30. Ask each participant to think of one person they would want a codeword with, and to say, out loud, what word or phrase they would propose. They do not have to commit to it publicly if they would rather choose privately. What matters is that the idea leaves the room as a specific plan attached to a specific person, not a general good idea they meant to act on. If the group is comfortable, ask two or three volunteers to share what they chose and why, since hearing a real example is what turns this from an abstract suggestion into something participants actually do that evening.

Part 03, the single action. Walk through the five numbered steps once, at a normal pace, then repeat step three alone: call back on a number you already had, never one given to you during the call. This is the step people get right in the room and forget under real pressure, so it is worth a second pass on its own.

Part 04, where to report. Read the numbers once. Do not linger. By this point in the session the room's attention is on the codeword they just committed to, not on phone numbers they can read off the handout later.

WHEN SOMEBODY SAYS THIS HAPPENED TO THEM

It will come up, usually during the exercise, sometimes as a general "this happened to my neighbor" and sometimes as a direct, current disclosure. Do not investigate it in front of the group and do not promise an outcome. Acknowledge it

plainly, thank them for saying it, and offer to talk afterward or connect them with the AARP Fraud Watch Network Helpline number on the handout. If money is actively at risk, say so directly and give them the "if money has already been sent" guidance from the module immediately, in front of the group if they are comfortable, or privately if not.

WHAT TO SEND BACK

Use the record on the following page, or simply write an email, to ayeniayomide5@gmail.com. Send nothing that identifies a participant: no names, no account details, no phone numbers that were actually used against someone. A pattern is enough where a pattern is what you have. The most valuable thing to report is not whether the session went well. It is any new variant of the scheme a participant described, because that is a pattern arriving in a community room before it arrives anywhere it can be measured.

DERIVED FROM

Module 03: AI-Generated Impersonation, and operational scheme characterization from the underlying detection work.

REVISION

Version 1.0, published June 30, 2026. The module: www.ayomideayeni.com

CORRECTIONS

Report a facilitation problem this guide does not address: ayeniayomide5@gmail.com

Ayeni, A. 2026. Facilitator guide, Module 03: AI-generated impersonation, version 1.0. Licensed CC BY 4.0.