Deepfake readiness drills: testing verification before a cloned voice calls



A new guide proposes a structured drill to show where verification fails when cloned voices or synthetic video calls target payments, help desk resets and access requests, with no real stakes.

- Cloned voices and synthetic video calls now appear in payment fraud, help desk resets and access requests.
- A structured drill shows security teams exactly where verification breaks down.
- The drill runs as a rehearsal, so nothing real is at stake.
- The article's example is a late Friday call that sounds like the CFO, asking a controller to release a supplier payment before the weekend.

The Hacker News describes a practical way to prepare for deepfake-enabled fraud: run a drill before an

attacker does it for real.

The risk

The article notes that cloned voices and synthetic video calls now feature in payment fraud, help desk resets and access requests. Its example is a call at 4:40 on a Friday from someone who sounds exactly like the CFO, asking the controller to push a supplier payment out before the weekend because a deal is closing. Urgency, authority and timing are the pressure points.

Why a drill

A structured exercise lets a security team see exactly where verification breaks down while nothing is at stake. Policies often assume staff will recognise a familiar voice or face; a drill tests whether the actual steps hold when that assumption fails.

What this means for institutions

The source excerpt is brief, so it does not detail the drill's format. The sensible reading for regulated institutions is to test the three areas it names: payment release, help desk identity resets and access requests. Each should rely on verification that does not depend on recognising a voice or appearance.

Results are most useful when recorded, assigned to owners and fed back into procedures and awareness training.

What to do now

1. Run a tabletop or live drill simulating a cloned-voice call requesting an urgent supplier payment.
2. Test whether help desk staff can be talked into identity or credential resets without independent verification.
3. Require call-back or secondary-channel confirmation, using known contact details, for payment and access requests.
4. Record where verification failed, assign owners and update procedures.
5. Brief finance, help desk and executive assistants on deepfake voice and video tactics.