Help desk verification script

Keep this by the phone. Use it for every request below, even when the caller sounds sure, senior or in a hurry.

Requests that always need verification

- Enrolling a new MFA device or phone number
- Removing MFA so the user can set it up again
- Any password reset on an account with admin roles
- Changing the recovery phone number or email
- Any request from someone who says they're new or traveling

Never verify with

- Anything the caller tells you (name, manager, employee ID, date of birth)
- The last four digits of an SSN or any detail that could be in a breach
- The number the caller is calling from, or a number they give you
- Caller ID, even if it shows a local or internal number

What to say

1. "I can help with that. For your security I'll open a ticket and call you back on the number we have on file."
2. If the phone on file is broken: "No problem. I'll contact your manager to confirm, or we can verify you on a video call."
3. If they push back: "I understand it's urgent. This check is the same for everyone, including executives. It'll only take a few minutes."

Then

1. Look the person up in the HR or directory system yourself.
2. Call back the number on file, or reach the manager through the directory.
3. For a lost phone: verify on video against the ID photo, or in person.
4. Issue a short-lived, one-time pass (for example a Microsoft Entra Temporary Access Pass). Let the user register their new method themselves.
5. Log the ticket: who called, what was asked, how you verified, who approved.

Stop and escalate to security if: the caller refuses a callback, asks you to skip a step, gives details that don't match the directory, or the same account had a reset request in the last 7 days.

Based on the HHS HC3 help desk alert (April 2024), CISA advisory AA23-320A and NCSC guidance (May 2025). From xcelcor.com/insights/help-desk-social-engineering.

From Xcelcor Guardian · xcelcor.com/insights/help-desk-social-engineering