Candidate Verification & Fraud Prevention Guide for Recruiters

This guide provides a structured approach recruiters should follow before scheduling an interview, to verify a candidate's authenticity and reduce the risk of fraudulent resumes or impersonation.

1. Check Digital Identity & Contact Consistency

Why: Many fraudulent candidates use temporary or AI-generated identities.

• Email domain check:
  - Use WHOIS or lookup tools (e.g., who.is, MXToolbox) to verify when the domain was created.
  - Flag anything less than 12 months old, especially if used for a personal or company domain.
• Cross-verify contact info:
  - Ask for a LinkedIn profile and confirm consistent job history.
  - Check phone number area code and require at least one voice or video confirmation before scheduling.

2. Verify Education and Employment Claims

Why: Fake resumes often omit graduation dates or reuse real companies with fabricated titles.

• Ask for graduation year and degree, and verify with the National Student Clearinghouse or the school registrar.
• Check for employment overlaps or implausible durations.
• Only accept professional references from corporate domain emails (not Gmail or ProtonMail).

3. Technical or Professional Plausibility Checks

• Request a portfolio, GitHub link, or project sample before the interview.
• Send a brief written or coding task that tests domain familiarity.
• Ask about specific projects ("What tool did you use for monitoring?") to ensure realistic responses.

4. Perform Background Validation (Ethically)

• Use LinkedIn reverse name search to find duplicates.
• Verify company or domain names in public business registries.

5. Require a Pre-Interview Voice or Video Verification

- Schedule a short video call to confirm identity and spoken communication.
- Request ID verification in accordance with HR policy.
- Confirm that their tone and experience match their resume claims.

6. Institutionalize a 'Candidate Verification Checklist'

Why: Reduces one-off mistakes and ensures consistency across recruiters.

Step	Verification	Red Flag
Email domain age	>12 months	Domain <6 months
LinkedIn presence	2+ years active	New or missing profile
Education	Verifiable	No graduation dates
Employment	Corporate reference emails	Gaps or overlaps
Voice/Video	Confirmed live	Refuses call
Portfolio	Provided & plausible	Generic or AI-generated
Resume metadata	Consistent formatting	AI polish or inconsistent fonts

7. Red Flags That Strongly Indicate Fraud

- Refusal to meet over video or voice
- Resume without education years
- Continuous or overlapping freelance roles
- Domain registered within past few months
- Overly generic accomplishments
- No LinkedIn activity before current year
- Prefers text-only communication (SMS, WhatsApp, Telegram)

Summary

These checks help recruiters filter out falsified or AI-generated resumes before scheduling interviews. Instituting a verification checklist ensures ethical, consistent, and defensible hiring practices.