

Job-Hunting Security Checklist

Use this checklist to validate employers, protect your data, and reduce risk during your job search. Review each section, check off items as you complete them, and keep records of your findings. When in doubt, pause and verify details using a second trusted channel.

Quick Company Verification Checklist

- ☐ Open the official company website and confirm the exact legal name.
- ☐ Find a physical address and match it on Google Maps, with street view if available.
- ☐ Check the Careers page for the same job title and description.
- ☐ Verify email domains match the website, avoid free-mail domains for official contact.
- ☐ Scan LinkedIn for company size, posts, and consistent employee histories.

Deeper Due Diligence

- ☐ Search recent news for leadership changes, funding, and product launches, verify dates.
- ☐ Look up domain age with a whois service, very new domains deserve extra caution.
- ☐ Read reviews on Glassdoor and Indeed for consistent patterns, not single anecdotes.
- ☐ Confirm business registration where applicable, match legal entity names.
- ☐ Validate recruiter identity on LinkedIn, look for tenure, mutuals, and activity.

Data Sharing Boundaries

- ☐ Do not share full date of birth, Social Insurance Number, or Social Security Number during screening.
- ☐ Do not share banking details or driver's license scans before a written offer.
- ☐ Provide only resume and portfolio until a conditional offer requires background checks.
- ☐ Offer to verify identity on-site, or via a secure third-party, after an offer is issued.
- ☐ Keep a log of what you shared, with dates and recipients.

Remote Role Safeguards

- ☐ Insist on official video platforms and calendar invites from company domains.
- ☐ Refuse to purchase equipment or gift cards with promises of reimbursement.
- ☐ Ask for written policies on equipment, onboarding, payroll, and security.
- ☐ Request a signed offer and contract before sending sensitive information.
- ☐ Confirm the team's location, reporting line, and regular working hours.

Email And Messaging Safety

- ☐ Treat urgency as a red flag, slow down and verify requests.
- ☐ Hover over links to inspect the real domain before clicking.
- ☐ Do not open unexpected attachments from unknown or mismatched senders.
- ☐ Ignore requests for passwords, two-factor codes, or payments over email or chat.
- ☐ Watch for domain lookalikes and spelling tricks, verify through a known channel.

Password And Account Hygiene

- ☐ Use a password manager to generate unique passwords for each site.
- ☐ Turn on two-factor authentication wherever possible.
- ☐ Never reuse passwords from email or banking on job portals.
- ☐ Consider a separate, professional email address dedicated to applications.
- ☐ Keep your browser, operating system, and antivirus tools updated.

Resume And File Safety

- ☐ Share city and province or state, not a full home address.
- ☐ Remove full date of birth and unrelated personal details.
- ☐ Export documents as PDF without embedded macros.
- ☐ Use expiring links with limited access when sharing portfolios.
- ☐ Name files clearly, include dates, and track who received them.

Money And Equipment Red Flags

- ☐ Legitimate employers do not ask you to prepay for software, equipment, or checks.
- ☐ Never deposit a cheque and forward funds to a third party.
- ☐ Decline requests for gift cards, crypto, or wire transfers.
- ☐ Wait for a signed offer before purchasing any equipment.
- ☐ Ask for written reimbursement policies and approved vendors.

People And Meeting Verification

- ☐ Confirm interviewer identities on LinkedIn and the company site.
- ☐ Request agendas and role titles on calendar invites.
- ☐ Verify office addresses on Google Maps before on-site meetings.
- ☐ Avoid private locations that do not match official office details.
- ☐ Share meeting details with a trusted contact for safety.

If Something Feels Wrong

- ☐ Stop, document everything, and disengage from the conversation.
- ☐ Capture emails, screenshots, file names, and source links.
- ☐ Report the listing to the job board or platform immediately.
- ☐ Notify the real company if their name was misused by scammers.
- ☐ Update passwords and place fraud alerts if sensitive data was shared.

Personal Scripts You Can Reuse

☐ “I am happy to provide additional documents after a formal offer is issued, including background check consent.”

☐ “For privacy reasons, I do not share government identification during screening, and can verify on-site or via a secure provider.”

☐ “I can share references after final interviews, and once we confirm mutual interest.”

☐ “Please send a calendar invite from your corporate domain, and I will confirm attendance.”

☐ “For security, I cannot purchase equipment in advance. Please share your written policy on equipment and reimbursement.”

Use Ai Agents For Faster Verification

- ☐ Ask an AI agent to compile official links, recent news, and leadership updates.
- ☐ Request dated milestones and flag unstable or contradictory details.
- ☐ Have it produce a verification checklist with links for manual review.
- ☐ Treat outputs as drafts. Always open and confirm sources yourself.
- ☐ Repeat the process for each employer to stay consistent and objective.