Guarding Your Career Search:
Navigating Security & Avoiding Scams Toolkit

September 23, 2025 Edition

By Jim McConnell
https://askmcconnell.com
Converged Security Services Provider

We provide a class on this topic to corporations, community groups, job seeker groups, HR professional groups. Contact us for scheduling.

Potential Indicators of Fraud / Scam

Understand that any one of these indicators may or may not identify the subject as a fraudster but more than one in the same interaction is almost certainly a brighter “red flag”. Be careful with (unconscious) bias and discrimination in any evaluation.

Fraudulent Recruiter		Fraudulent Job Seeker	
Potential Indicator		Potential Indicator	
□	LinkedIn (or other platforms) – Has the Profile been open for many years but very small number of followers?	□	Did job seeker provide an unsolicited resume, maybe even demanded you forward or enter into your talent community/ATS?
□	LinkedIn (or other platforms) – Is the Profile old, but the profile picture been modified in the last week or two?	□	Are there indications person is using Fake IDs? (Passport doesn’t match the DL, for example)

☐	Does the Messages/Texts contain questions like “Have we met recently?”, “Do I know you?”	☐	Is the job seeker hesitant about live calls or video calls and only wants to leave voice messages or audio attachments? Could be using voice cloning
☐	LinkedIn – Messenger – Does the message make a statement like: “I don’t know why LinkedIn keeps recommending you?”	☐	Does job seeker refuse to turn off any video/image backgrounds when interacting via a video call?
☐	Do they send a couple of introduction messages/texts and then ask you to move to WhatsApp, Telegram, etc.?	☐	Is the job seeker’s watch, PC clock or clock in room showing a different time than expected? (ask to see clock). Address on paperwork is Dallas Fort Worth (Central Time Zone) but clocks are >1-2 time zones different?
☐	Do they talk about “working on a project that your skills would be great for”, but won’t tell you anything about the project?	☐	Does it appear/sound like a dual person interview? (One answers, different person, in a chat or ear bud is giving the first person the answers). Watch the eyes, touching the ears, looking away a lot
☐	Common jobs: Are they in the “Import/Export business” or “Jewelry” or “Medical” or “Energy”	☐	Did a different person show up for onsite interview and/or on the first day then who was interviewed or ID’ed?
☐	Do you/they request a video interview/call, but then at the last minute, “my camera isn’t working”?	☐	Does the job seeker agree to a video call but at the last-minute mention “my camera isn’t working”? “Contact me back when you get your camera working…”
☐	Do they do a generic introduction messages/texts and then when you ask for details, they tell you their boss will have to send you the details of the job (usually via WhatsApp)?	☐	Does the job seeker complain about the ATS or that it isn’t working and asks you to fill in the ATS information for them? They are trying to avoid ATS details and terms and conditions.
☐	Is the job description they send you, in plain text email with little introduction?	☐	Is the job seeker heavy name dropping beyond casual acquaintance or referral?
☐	Is the email / job description have the majority of email is in lowercase?	☐	Not specific to a specific job seeker, but are you getting a high volume ATS submissions (from same IP address)?
☐	Is the “From:” Email address a name/word followed by some numbers: name[numbers]@someemailservice[.]com like Gmail or iname or Yahoo? Did you get additional emails on the same job or similar job the same day or next day but from a different name+[numbers] email address?	☐	Does the resume show exact terms/phrases in resume that are usually copy pasted from the job description? (particularly from the “Required” section)
☐	Did 2-3 different “analysts” try to recruit you for the same job by the same recruiting company?	☐	Is the language/dialect of resume match candidate’s home/native country/language (AI involved?)
☐	Is the recruiter work for or is the job for a company that has a generic consulting/recruiting website with no specific information on leadership, legal status, privacy policy?	☐	Does the Caller ID on any phone calls match company phone number (range)? Obviously with cell phones this

			isn’t always possible, but a good check when getting official calls
□	Is the recruiter’s company or job for a company that is on LinkedIn with: • unusual employee title mix • little to no employees, no logo, posts, etc. or • very large volume of employees that doesn’t match website/HQ building	□	Is the job seeker wearing a mask on video calls? Rare in a Post-COVID world, especially if they the background appears to be a residential home.
□	Does the messages/text or email talk about “reviewed your profile/resume” or “wanting to learn from you”, but you are in accounting, and they are in export business, jewelry design or some other odd mismatch role/field?	□	Are any email addresses in the cc: line pointing to generic website addresses (e.g. Gmail, iname, Yahoo, etc.)?
□	Do the messages/texts appear to be immediately personal? Like: “Want to meet for pizza today?”….”This isn’t Mary?”….”I am so sorry to bother you”….”Where do you live, I enjoy meeting people?”	□	Is the job seeker not familiar with what your company does? Especially if large, well-known brand?
□	Does the messaging talk about “We have reviewed your profile / resume”, but the role they are “recruiting” has nothing to do with your skills? (e.g. You’re a supply chain director, but they are recruiting for a call center)	□	Does the job seeker ask something about “which job is this about”?
□	Does the message/text/email talk about “Part Time work”? Particularly “helping improve customer satisfaction / product review scores”?	□	Is the Flesch-Kincaid Grade Level of the resume unusually high or unusually low for the role?
□	After setting up video call, you ask them to turn off their background image, but they refuse to do so?	□	Do they want to meet at an unusual location vs. company office or public place Starbucks?
□	Does the person name drop of who you might know or who they work for?	□	Does their LinkedIn Profile “# of Connections” also appears as a URL/Link?
□	When you mention you know someone at their company or will call a person at their company, do they immediately talk about that they used to work there?	□	Education (degrees) listed on LinkedIn vs. Resume/CV vs. Application don’t match. LinkedIn is used for SEO, Application usually is most accurate as they are agreeing it is accurate with consequences.
□	When you look up the phone number (e.g. text, caller ID, email signature) from “company” does it point to company in a internet search?		
□	Do they refuse or try to redirect any communications you initiate to the company?		

□	Do the offer to “Just send me your resume” and I will help complete the ATS work?		
□	Does the individual (“recruiter”) say something like, they are ready to hire on the spot and “No interviews necessary”, just send me your paperwork (Resume, PII, etc.)?		
□	Does the message/text talk about “Can we meet for coffee next time I am in (your home city)”, but build not professional relationship?		
□	Is the recruiter wearing a mask on video calls? Rare in a Post-COVID world, especially if they the background appears to be a residential home.		
□	Are the email addresses in the cc: line pointing to generic website addresses (e.g. Gmail, iname, Yahoo, etc.)?		
□	Is the communications talking about a “New company” / “New project” they can’t provide any details without you provide more (sensitive) information or money?		
□	Is the “recruiter” asking for money, SSN, copy of ID (before interviews or sometimes during interviews)?		
□	Does the recruiter / company’s website use a generic legal / privacy notice (if one exists at all)? Look for legal/privacy language that is irrelevant or lacks contact information.		
□	Is any physical/mailing addresses (if any exist) on website point to a generic mailbox (USPS, UPS Store, Mailboxes Etc, for example)?		
□	Is the posting on legitimate job board but with odd company information (“Jake’s Recruitment”, “Confidential”, etc.)?		
□	Does the recruiter advise you need to take some training or “personality test” before interviews (with or without cost)? These tests tend to collect a lot of personal information directly and indirectly.		
□	Does the posting / recruiter promise “High Pay” for “work from home” / “work anywhere” but it is call-center type of work?		
□	Is the recruiter requiring you to complete a background check BEFORE interviews or offer discussions?		
□	Is the job posting / recruiter (instructions) requiring you to scan a QR codes and/or download Cell Phone Apps needed for the		

	application or interview? “We use a special version of [name of common app]”		
□	Are the emails from the recruiter missing a classic business email signature?		
□	Does the recruiter showing up with multiple LinkedIn profiles and/or the one in their email signature does not work?		
□	Does the From: lines in email not match email signature or normal email format or domain for that company?		
□	Do they want to meet at an unusual location vs. company office or public place Starbucks?		
□	Does their LinkedIn Profile “# of Connections” also appears as a URL/Link?		
□	In their recruiting / interview process are they asking you to download their “tool”?		
□	Are the asking you to “sign” an exclusivity agreement? “I Agree” email		
□	Do they reach out to you in a Comment thread about helping you or an offer or job that has little to nothing to do with the Thread? Or event when you announce you got a new job, they are looking to help you find another job…..		
□	Do they recommend someone to help you or a group and refer you to a common email address (e.g. Gmail) but no other contact information like a LinkedIn profile or website, etc.		
□	Does the job seeker “helper” claim they are “retired” and do they have a website, LinkedIn profile, phone number, contract, EIN, W9, etc.?		
□	Does the profile and/or banner picture look “staged” / out of sorts for the role, name, culture of the company? “Too Pretty”? “Too Vacation” looking.		
□	You add on the “Open For Work” Banner and your get (semi-)instantly flooded with offers from “Recruiters”. (P.S. I still think the value of this banner outweighs the Fraudster exploitation of it, but be careful)		
□	Does the recruiter show THEY are unemployed in their profile?		
□	Claims to be a broker of recruiters and just sends screen shots of jobs headers		

□	Talking about a “New Project” that doesn’t fit their company or title (Chef Baker with a new AI project)		
□	Is their email domain have letters or a nexus in spelling to the company they are supposedly recruiting for? (e.g. Acme Brick Company being abchr.com or abcrecruit.com)		
□	Is the “assistant” or person communicating with you, using the name of real HR employee of the company they are supposedly recruiting for?		
□	Is the job description they send you not viewable on any website or career page? And does it look TOO perfect like they copy elements from your resume or LinkedIn Profile (using AI)?		
□	Offering / Sending you a check for “Equipment Setup”		

Integrity Check Ideas

These are all good practices, but there is no need to pour on these with a candidate/recruiter if they haven't provided significant indicators from the previous section

Scam Resistant Recruiter		Scam Resistant Job Seeker	
Integrity Checks of Job Seeker		**Integrity Checks of Recruiter**	
□	Require real live backgrounds on Video Calls	□	See if recruiter is LinkedIn Verified via CLEAR, if not and you are suspicious, ask them to get Verified before the interview (takes like 15 minutes most of the time)
□	Use passport for verification or combination of passport and DL	□	Require all emails to come from company domains vs. gmail.com/yahoo.com
□	Use wet ink signature and compare to passport / DL	□	Don't pay any fees or requests for gift cards or provide any bank/credit card/Zelle/Venmo-type of information
□	Ask the job seeker to show you a clock and their watch and denote the time (difference)	□	Ask for formal email from hiring company for interviews
□	Check LinkedIn profile (Contact Info and "About This Profile") for recent changes (picture, profile, # of followers, etc.)	□	Require real backgrounds of recruiter on video calls
□	Ask about very specific item on their resume	□	Unless you are at the offer stage and have met with them face-to-face, avoid SSN or other sensitive / financial information sharing.
□	Check the phone number on resume, LinkedIn, or ATS application to see if they are using a foreign phone number but have been in current country for many years	□	Provide references requests later in process (otherwise your references become assets/targets)
□	Work with ATS vendor on technology-based detection (GeoIP of Applicants, Volumetric Controls, Source URL Controls	□	Watch out for plain-text emails
□	If candidate is overseas, legitimately, schedule the interview in YOUR time zone to see the response	□	Watch out for people cc'ed (gmail, yahoo, foreign) – Be careful with "Reply-to-All"
□	Ask about conflicting information based on a LinkedIn/Resume specific item	□	Ask the recruiter to show you a clock and their watch and denote the time (difference)

Resource by Jim McConnell from AskMcConnell.com

□	Ask same question via email and interview and see if what they put in writing or talked to is significantly conflicting	□	Check LinkedIn Profile (Contact Info and “About This Profile, number of followers, etc.) of the person and their company
□	Verify LinkedIn Profile, Resume/CV, and Application all match	□	Do due diligence on company (recruiting firm and/or hiring firm). “Can’t tell you who the client is?” Possible red flag, advise you need to review who the client is for conflict-of-interest checks with your legal counsel.
□	Onboarding / Laptop Shipping to different address then government documentation	□	Don't click on links or send documentation via email without good due diligence on the links and ask.
		□	Scrutinize the recruiter’s signature blocks
		□	Check for non-working LinkedIn profiles or recruiter and company
		□	Watermark PDF’s of Resumes with Company Name – This can break SOME ATS, so this might only work if you are email a legitimate recruiter your resume directly.
		□	Consider the statement: “I’m not legally allowed to use WhatsApp/Telegram”
		□	Do not engage with obvious fraudster, just block, report, and move on
		□	Thoroughly review the official websites of the recruiter and hiring company
		□	Thoroughly review the LinkedIn profiles of the recruiter and hiring company
		□	Check out employee reviews on platforms like Glassdoor. (Be aware these reviews can also be fraudulent)
		□	Check if a company is registered with business directories like BBB, CorporationWiki, OpenCorporates
		□	Review LinkedIn “Current Employee” lists (Filter using “Current Company”
		□	Review the website’s Terms and Conditions and Privacy Policies
		□	Look like the company’s DUNS information and Secretary of State (may be a small fee, but worth it.
		□	Do NOT use Auto-Appliers
		□	Just because the reach out is in a chat, comment stream, video call chat stream, doesn’t mean is can be trusted.

Resource by Jim McConnell from AskMcConnell.com

		□	If job is on LinkedIn, the “Verified” icon, is a good indication of a “real” job. But only 50% are “Verified”, which doesn’t mean the other 50% AREN’T legit, this icon is just another GOOD indicator.
		□	Be careful about applying through Job Aggregators aka “Job Search Engines” especially ones that post jobs on regular job sites like LinkedIn under their name vs. the hiring company’s name.
		□	Required them to email you from the domain of the company’s website
		□	Check date website domain was created
		□	Do a Google Reverse Image search on recruiter’s LinkedIn photo

Other Identity Security suggestions you should consider implementing for: you, your family, and your business

Domain	Example of Actions	Personal	Family
Background Checks	Of your personal service providers (e.g. “Handyman”)	✅	✅ (Kidding)
Email Security	Gmail: https://support.google.com/accounts/answer/46526?hl=en Office 365: https://learn.microsoft.com/en-us/microsoft-365/community/basic-security-set-up-for-microsoft-365 Yahoo: https://help.yahoo.com/kb/SLN2080.html Apple iCloud: https://support.apple.com/en-us/108756	✅	✅
Employee Training / Family Training	https://www.knowbe4.com/free-cybersecurity-tools/phishing-security-test	✅	✅
(ID) Theft	https://lifelock.norton.com/products/budget-friendly	✅	✅
Computers	Yearly clean up, backup, Lock down security / privacy settings	✅	✅
Cell Phones	Yearly clean up, backup, Lock down security / privacy settings	✅	✅
Social Media	Yearly clean up, Lock down Privacy Settings	✅	✅
Virtual Credit Cards (sorry Dave Ramsey), Apple Pay, Google Pay	Majority of major credit card providers offer a web / app based option to use a Virtual Credit Card	✅	✅
Three Credit Reports	Put it on your calendar to pull every 4 months	✅	✅
Shredder	Cross Cut Shredder from Amazon	✅	✅
Sentence Passwords	!CowJumpedOverTheMoon2025!	✅	✅
Electronic Communications/Documents	https://bunkr.life/	✅	✅
AntiVirus Software	https://www.tomsguide.com/us/best-antivirus,review-2588.html	✅	✅

Resource by Jim McConnell from AskMcConnell.com

Password Manager	Apple, Microsoft, Android tools where possible otherwise, see the latest reviews from reputable publication: https://www.macworld.com/article/668938/best-password-managers-2.html	✅	✅

Example ChatGPT AI Prompt – Questionable Recruiter Due Diligence

“Research [Company Name] and determine if a recruiter named <recruiter’s name> and job listing <insert job title> associated with it is legitimate or potentially a scam.

Check for:

Official company website and job board listings.
Presence of the recruiter on LinkedIn or other professional platforms.
Known scams or fraud alerts related to the company or job title.
Consistency in job listing details across trusted job boards (e.g., LinkedIn, Indeed, Glassdoor).
Any red flags such as upfront payment, use of generic emails (e.g., Gmail/Yahoo), poor grammar, new website/domain or urgent/luxury offers.

Summarize findings and give a likelihood rating (High, Medium, Low) of legitimacy based on available data “

Resource by Jim McConnell from AskMcConnell.com

Chief Security Officer / Chief Information Security Officer / General Counsel / Chief Human Resources Officer Responsibilities

	Role	Recommendations
□	CHRO	Make sure your career page has a PSA about these types of scams and how best to communicate with your HR team if they don’t know if something is a scam or not
□	CISO	Make sure ATS and Career Page logs flow into your SIEM and monitoring/alert on them
□	CHRO/CISO	Make sure your ATS has implemented all the enhancements mentioned below
□	GC/CHRO	If you outsource any part of your hiring, make sure the contract covers these types of fraud/scams and security enhancements mentioned in this resource
□	GC	Make sure your supply chain/supplier/vendor/third party contracts include protections from their types of frauds/scams (Flow Down also)
□	CISO	Watch your PassiveDNS logs for recruiting domains
□	CISO/CHRO/GC	Make sure you add training on this topic to your legal team, HR team, contracts teams required training
□	CHRO	Assign someone on your team to audit the LinkedIn “Associated Members” list monthly, at a minimum

Applicant Tracking System (ATS) Enhancements and Security Settings

If you work for an ATS manufacturer or your company has built its own ATS, these enhancements can significantly improve the security of your Recruiting / Talent Acquisition program

If you outsource your ATS, these should be added to your contract as ADDITIONAL security requirements to be implemented by your ATS Supplier

ATS Security Enhancement Description / Setting
Limit applicants to certain GeoIP (basic on job country, or high risk countries)
Block IP Addresses or blocks of IP Addresses from applying
Support a Coss-ATS industry IOC IP/email block list
Ability to stream ATS (login, email, transactional) event logs to common SIEM's / SIEM formats
Ability to flag / notify clients when applicants based on high velocity login or application submission
Allow for uploading of headshot (require by default)
Allow for upload of photo ID (require by default)
Allow for comparison of photo ID to headshot (require by default)
Ability to search and alert on job descriptions that are on platforms not specific pushed to via the ATS.
Support 2MFA for all users, (require by default)
Ability to red flag applicant where their email, phone, IP address isn't the same country
Ability to detect, alert and block on referral codes being misused
Ability to detect, alert and block on referral employee information being misused
Ability to support CAPTCHA before submission (require by default)
Ability to have support Red Flag indicators
Ability to support a ATS developed or client development AI LLM to detect fraudulent applications
All logs (see #004 above) include IP address whether from login, transaction actions, email (pull from SMTP headers) tracking, etc.
Have Red Flags alerts where IP address is known (industry) AUP violator or email domain
Ability to scan attachments and any included URLS through tools like VirusTotal
Ability to check the submitted resume looking for partial duplicate resume content across applicants/jobs.

Resource by Jim McConnell from AskMcConnell.com

Good Desktop / Laptop Antivirus / AntiMalware Summary (from Matt Keelan on 7/7/2025)

🛡️ Popular Antivirus Programs That Scan Email for Scams

Antivirus	Email Scam Protection Features	Notes
Bitdefender Total Security	✅ Anti-phishing, fraud detection, and email scam filters	Strong real-time filtering; works with most clients
Norton 360	✅ Email scam detection and phishing protection	Detects dangerous links & attachments
McAfee+ Premium	✅ Anti-phishing and spam email scanning	Real-time link & scam detection
Kaspersky Premium	✅ Mail Anti-Virus scans incoming/outgoing messages	Supports full mail protocol scanning (POP3, IMAP, SMTP)
ESET Smart Security	✅ Email client protection (e.g., Outlook, Windows Mail)	Detects malicious attachments and URLs
Trend Micro Internet Security	✅ Blocks email scams, phishing, and malicious links	Strong webmail & social platform filtering
Avast Premium Security	✅ Email shield scans email attachments & blocks dangerous links	Free version has limited email scan features
AVG Internet Security	✅ Similar to Avast; includes email scanner and link scanning	Good for basic scam detection
Sophos Home Premium	✅ Web and email threat detection using AI	Business-grade tech in a home product
Malwarebytes Premium	❌ No direct email scan, but detects threats if links/files are clicked	Best used alongside other AV tools

🧠 Key Points

- Most tools **do not scan webmail (Gmail, Yahoo) directly**, but:
    - They **analyze links and attachments** when you click them.
    - They often include **browser extensions** to detect phishing attempts.

Resource by Jim McConnell from AskMcConnell.com

- For **desktop email clients** (like Outlook), many AVs **scan messages in real time**.
- Products like **Bitdefender, Kaspersky, Norton, and ESET** are known for **top-tier email filtering**.

✅ **Recommendation:**

If email scam prevention is a priority, consider:

- **Bitdefender** – Excellent email and web phishing protection.
- **Norton 360** – Great for families and all-around security.
- **ESET** – Light on system resources, strong mail client scanning.
- **Kaspersky** – Very detailed email protocol scanning (POP3/SMTP).