Staff OS — Fraud Awareness

Protecting Candidates from Recruitment Fraud

Staff OS is built on the belief that every candidate deserves a respectful, transparent hiring experience — powered by technology they can trust. We want to make sure that anyone engaging with our platform or exploring opportunities through our Clients is protected against fraud, phishing, and impersonation attempts.

Unfortunately, bad actors sometimes misrepresent themselves on job posting sites, social media, and messaging platforms — posing as recruiters or representatives affiliated with Staff OS or our Clients. Below are guidelines to help you identify legitimate Staff OS communications and protect yourself.

How to Identify Legitimate Staff OS Communications

- **Official Email Addresses:** Any recruitment-related outreach from a Staff OS employee will be sent from an **@staff-os.com** email address — never from generic email providers such as Gmail, Outlook, Yahoo, or similar services.
- **AI-Powered Conversations:** When you interact with our AI recruitment platform, you will be clearly informed that you are communicating with an automated system. Legitimate AI conversations through Staff OS will occur through verified platform channels — including designated SMS/MMS numbers, web chat interfaces, or integrated job board messaging — not through personal phone numbers or social media direct messages.
- **Client-Branded Interactions:** In many cases, you will interact with our platform under a Client's brand (the company you are applying to). Legitimate conversations will reference specific job opportunities and will not ask for sensitive personal or financial information outside of a formal, secure application process.

What Staff OS Will Never Ask You to Do

During the recruitment process, Staff OS and our AI platform will **never** ask you for the following:

- **Financial account information** — including bank account numbers, credit card numbers, wire transfer details, or cryptocurrency wallet addresses
- **Government-issued identification numbers** — such as Social Security numbers, Social Insurance Numbers (SIN), driver's license numbers, or passport numbers — outside of a formal, secured onboarding process
- **Passwords** — to your email, social media, financial accounts, or any other service
- **Payment of any kind** — including application fees, processing fees, background check fees, equipment charges, training costs, or inventory deposits. You should never have to pay to apply for

or obtain a job.

- **Management of financial transactions** — such as receiving, transferring, or withdrawing funds on behalf of a company or individual
- **Shipping or receiving packages from your home** as a condition of employment
- **Acting as a financial intermediary** — including forwarding payments, purchasing gift cards, or facilitating money transfers

---

Red Flags to Watch For

Be cautious if you encounter any of the following:

- An "offer" of employment without a formal interview or application process
- Communication from a generic email address (e.g., staffos.hiring@gmail.com) rather than an official @staffos.com address
- Pressure to act quickly, provide personal information immediately, or make a financial commitment
- Requests to communicate exclusively through personal messaging apps (WhatsApp, Telegram, etc.) rather than official channels
- Job postings that promise unusually high compensation for minimal work
- Requests to download software or click links from unverified sources
- Messages with poor grammar, spelling errors, or formatting inconsistent with professional communications

---

Reporting Suspected Fraud

If you receive outreach from someone claiming to represent Staff OS or a Staff OS Client that seems suspicious, involves any of the requests listed above, or otherwise does not feel legitimate, please report it immediately:

- **Email:** security@staff-os.com
- **Subject Line:** "Suspected Recruitment Fraud"

Please include as much detail as possible, such as the sender's name, email address or phone number, the content of the communication, and any screenshots.

Additional Resources

You can learn more about protecting yourself from online fraud and recruitment scams through the following resources:

- **Federal Trade Commission (FTC):** consumer.ftc.gov — guidance on recognizing and reporting scams
- **Internet Crime Complaint Center (IC3):** ic3.gov — a partnership between the FBI and the National White Collar Crime Center for filing online fraud reports
- **Canadian Anti-Fraud Centre (CAFC):** antifraudcentre-centreantifraude.ca — Canada's central agency for collecting information on fraud and identity theft
- **OnGuardOnline:** onguardonline.gov — tips from the federal government on staying safe online

---

Your safety matters to us. If something doesn't feel right, trust your instincts and reach out. We'd rather investigate a false alarm than see a candidate harmed by a scam.