

# Identifying Job Scams

## Our Commitment To Your Career Safety

Does a recent job opportunity seem too good to be true? Job scams are becoming increasingly sophisticated as malicious actors continue to refine their tactics. To stay safe while advancing your career, it is essential to recognize job scams usually unfold in stages, much like a legitimate hiring process.

There are five primary "stages" where a scammer might try to trap you, from the initial outreach to the final (and most impactful) financial request. Learn to quickly identify these common job scams to keep yourself safe while building your career.

**At EchoStar, we look forward to meeting our future team members and establishing a genuine connection! Our hiring process involves multiple touchpoints, using phone and video conversations to establish mutual trust, and providing the candidate ample time to review the offer at hand.**

### Brand Mirroring

Scammers not only create fake job posts, but have also become proficient at 'mirroring' reputable companies to gain your trust. These malicious actors often browse the internet to find the names and titles of actual hiring managers or HR leadership. They further the fraud by using high-quality logos, official-looking letterheads, and additional corporate branding and messaging in an effort to 'validate' their identity. While scammers may mimic brand messaging, they often cannot hide their email source. Watch for 'look-alike' domains that include extra hyphens or words to appear official. If an outreach comes from a public provider, like Gmail or Outlook, it is often a sign of a job scam.

### Early Collection of PII

In the early stages of your interview process, sometimes even before an initial interview, scammers may attempt to steal your Personally Identifiable Information (PII) using the pretense of background checks. PII can include sensitive information such as your driver's license number, social security number, home address, and much more. Legitimate employers will only request this sensitive information through secure portals *after* a formal offer has been sent and signed.

### Chat-Only Based Interview

Malicious actors typically avoid face-to-face, video, or voice interaction interviews, as it is harder to maintain a fake persona for job scams. To bypass the need for visual identity, the interview process may be held over messaging apps such as WhatsApp, Telegram, Signal Gchat, or Teams. Conducting interviews solely through messaging apps allows malicious actors to hide behind a stolen headshot, fake name, and scripted,

## Identifying Job Scams

corporate-style responses, making the interaction feel trustworthy. Once a scam is successful, the chat history can be easily deleted or the scammer can block the victim, leaving no paper trail for your bank or local authorities.

### **Rushed Offers**

Having a quick turnaround during the interview process may sound enticing, however, it poses a large risk. One of the most common tactics of these job scams is an unnaturally fast timeline, creating a sense of urgency in candidates. The intent is hoping the victim will sign documents or share data before having a chance to spot inconsistencies. Malicious actors create a false sense of urgency, often stating the position must be filled immediately or requiring the offer to be signed within the hour. This tactic is designed to trigger a fear of missing out.

### **Check Reimbursement Trap**

Financial reimbursement for home-office equipment is one of the leading financial tactics for job scams. The scammer, posing as a hiring manager, sends a digital check to the candidate once the 'offer' is received. From here, the candidate is instructed to deposit the check and use those funds to pay a certified vendor for the equipment. Many fall victim to this tactic as the balance may briefly appear in the account, however, once the bank discovers the check is fraudulent, the deposit is reversed and if the money has been sent to the 'vendor', it is gone from your personal account forever.

### **Prioritizing a Secure Search**

At EchoStar, we are committed to maintaining a transparent, secure, and human-centric hiring process. By staying informed about these common tactics, you can proactively protect your personal information while navigating the job market confidently.

If you suspect you are being targeted by someone impersonating a member of the EchoStar recruiting team, or if you encounter a suspicious job listing, please reach out to our hiring team at [recruiting@dish.com](mailto:recruiting@dish.com).