OUCH! August 2025

SANS SECURITY AWARENESS

Spotting Online Job Scams

Maria's "Dream Job" that Turned into a Nightmare

Maria had just completed her community college degree and was eager to land her first full-time remote job. So, when she received a message on LinkedIn from someone claiming to be a recruiter for a global tech company, she was thrilled. The job was for a "Remote Administrative Assistant"—$4,000 a month, flexible hours, and all equipment provided. The recruiter said her profile was impressive and wanted to fast-track her for an interview.

The interview happened the next day—over a messaging app. It felt a bit odd, but the recruiter explained that the company was transitioning to be fully remote. After a quick 20-minute chat, Maria was told she got the job. Then came the next steps: She needed to fill out onboarding paperwork, including her Tax ID number, bank information, and a photo of her driver's license for HR records.

A few days later, she received a check for $5,000 to purchase a laptop and software. She was instructed to deposit the check and then send $3,800 via bank transfer to their "approved" laptop supplier and keep the remaining money for additional expenses.

Maria followed the instructions—but three days later, her bank contacted her. The check was fraudulent. Maria not only lost money, but she also shared highly sensitive information that would most likely be used for identity theft. Her excitement about a new career opportunity had blinded her to the warning signs.

How Job Scams Work

Job scams are effective because they exploit your emotions and urgency. If you're unemployed, under pressure, or just excited about a promising opportunity, it's easy to overlook warning signs. Scammers also use professional-looking emails, websites, and even spoofed phone numbers to appear legitimate. They often begin by creating convincing listings on social media, often for remote or flexible positions. They then reach out to you via email or perhaps message you offering you a job. These scammers often pretend to represent real companies to gain your trust. After some back-and-forth communication, scammers might conduct a fake interview via email, text, or chat apps. The "job offer" soon follows.

Their end goal is to get your money, As in Maria's case, or obtain your highly sensitive information so they can steal your identity and commit fraud in your name.

Red Flags to Watch For

Despite these scams being increasingly sophisticated, there are consistent red flags you can watch out for.

- **Too Good to Be True**: Extremely high pay for little work, immediate job offers without an interview, job offers that are clearly above your qualifications, or promises of fast hiring.
- **Pressure to Act Quickly**: Scammers want you to commit before you have time to think or research.
- **Vague Job Descriptions**: If the job posting is unclear or overly generic, be cautious. Legitimate employers usually provide detailed descriptions and required qualifications.
- **Requests for Payment**: You should never have to pay for job training, background checks, or equipment up front.
- **Odd Communications**: Be very suspicious of offers from Gmail, Yahoo, or similar personal email domains. Legitimate recruiters typically use corporate email accounts. Look out for overuse of messaging apps and avoiding phone or video calls. Always use extra caution for communications that you did not initiate.
- **Hidden Company Information**: If you can't find the company online, or its website, LinkedIn profile, or online presence looks suspicious, proceed with caution.

How To Protect Yourself

You can still take advantage of online job opportunities while staying safe–just take a few precautions:

- Always verify the employer through independent searches and visit the company's official website and confirm that the job is listed there.
- Stick to reputable job search websites and professional networks. They are less likely to have job scams, but they can still happen.
- Never provide your Tax ID number, bank details, or copies of your ID during initial conversations.

Ultimately if something feels off, it probably is. Take a step back and consult someone you trust. The greater the sense of urgency and the greater the opportunity, the more likely it is a scam.

Guest Editor

Donna Ross is Executive Vice President and Chief Information Security Officer at Radian. With over 25 years of experience in cybersecurity, compliance, and enterprise risk management across multiple industries including finance, healthcare, insurance, and manufacturing, she leads Radian's information security, risk mitigation, and privacy functions–focusing on strategy, resilience, and governance.

Resources

Romance Fueled Investment Scams: https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Account Takeovers: Emotional Predators: https://www.sans.org/newsletters/ouch/account-takeovers-emotional-predators/