Phishing Careers

An email about a job opportunity just begs to be opened. Criminals know this, so they'll send emails with enticing subject lines and content designed to get you to click malicious links. Be wary of career-related phishing emails that provide lots of excitement but little detail. Phrases like, "You're hired" and "No experience necessary" or "High salary guaranteed" are red flags, and a sure sign the email should be avoided. Another scammer trick is to mimic popular job search and networking platforms, like Monster, Indeed, LinkedIn and others. Pretend emails asking you to download job details from these sites should be regarded carefully. Look closely for grammar mistakes or graphics that don't quite measure up. Sender names, addresses and urls that don't match the platform name are also a sign of potential problems. If anything seems off, refrain from downloading attachments or clicking links. Do not respond as this lets the scammer know your mailbox is active, meaning you'll be targeted again at some point. To verify if a job opportunity is legitimate, go directly to the site by keying in the web address and using the search function.

If you're a human resources associate or hiring manager, you're especially appealing to cybercriminals because your job depends on processing outside information. You also possess a significant amount of personally identifiable information, or PII, that scammers can use to steal identities. While you can't prevent being targeted, you can harden your stance against cybercriminals by being extra vigilant. Even a simple email with the subject line 'my resume' or 'references' could be the source of a crippling ransomware attack that shuts down your network. Develop a healthy skepticism, and verify emails before clicking links or downloading by contacting the applicant directly. In addition, work with information technology to ensure your security software is up to date. If you're part of a larger group in charge of hiring, route incoming applications through a single workstation that's isolated from the network if possible. This way, if something malicious does get in, it can't impact the company network and the unit can be reset.

Barracuda
Your journey, secured.