



Protecting candidates from recruitment scams

Black & Veatch has become aware of **unauthorized individuals impersonating our recruiters** and contacting job seekers. These individuals may attempt to obtain personal information or direct candidates to third-party services.

Your safety and trust are important to us. Please review the information below to help you recognize and avoid fraudulent activity.

How Black & Veatch recruits

Black & Veatch recruiting processes follow consistent and verifiable practices:

- Our recruiters will **only communicate using official Black & Veatch email addresses (@bv.com)**
- All open roles are posted on our official careers site
- Our process includes formal interviews and direct communication with our team
- We do not require payment or third-party services at any stage of the hiring process

Warning signs of a potential scam

Be cautious if you encounter any of the following:

Unverified communication

- Emails from personal accounts (e.g., Gmail, Yahoo) claiming to represent Black & Veatch
- Messages from profiles that do not clearly align to verified Black & Veatch employees

Unusual requests

- Requests for payment, resume services or application fees
- Requests for sensitive personal information early in the process (e.g., banking information, identification documents)

- Offers that skip standard interview steps or appear unusually urgent
- Being asked to communicate outside of professional channels

Recruitment scams often mimic legitimate hiring practices and may reference real job postings or employee names, so it's important to verify before proceeding.

What you should do

If you believe you have been contacted by someone impersonating Black & Veatch:

- Do not respond or provide information
- Verify the opportunity by visiting our official careers page
- Report the interaction to Black & Veatch at: HRCareersTechSupport@hrsupport.bv.com

Our commitment

Black & Veatch is committed to protecting candidates and maintaining a secure hiring process. We actively monitor and respond to impersonation attempts and work with external platforms to address fraudulent activity.

If you are unsure about communication, we encourage you to pause and verify before acting.