Fraud Alert

Be aware of scams involving phony job postings.

There have been a number of instances where fraudsters have been posing as Xylem recruiters or Human Resource representatives in the marketplace. People have been offered fake jobs with Xylem. We take this matter seriously, and are working with the appropriate authorities to effectively address the issue. By making you aware of this, we hope to avoid, and ultimately prevent, unsuspecting individuals from falling victim to this scam.

What is recruitment fraud?

Recruitment fraud is a sophisticated scam offering fictitious job opportunities. This type of fraud is normally perpetrated through online services such as bogus websites, or through unsolicited e-mails claiming to be from the company. These emails request that recipients provide personal information, and ultimately payments, to process applications, purchase equipment, or a variety of other things, for jobs that do not exist.

How to identify recruitment fraud?

- Monetary or check cashing requests as part of the hiring process. These types of requests are never part of any legitimate hiring process at Xylem. In some cases, they may send you a check to deposit, then inform you they have overpaid and will request a partial refund from you.
- The fraudsters may conduct the entire process over email, but will often ask recipients to complete bogus recruitment documentation, such as application forms, terms and conditions of employment or visa forms. The Xylem name and logo might fraudulently be featured on the documentation.
- There is an early request for personal information such as address details, date of birth, resume / CV, passport details, bank details, etc.
- Candidates may be requested to contact other companies/individuals such as lawyers, bank officials, travel agencies, courier companies, visa/immigration processing agencies, etc.
- E-mail correspondence is often sent from (or to) free web-based e-mail accounts such as Yahoo.com, Gmail.com, Googlemail.com, Live.com, etc.

- E-mail correspondence appears to be sent from an officer or senior executive of the company, often in Legal or Human Resources. If the email address doesn't end with "@xyleminc.com" it most likely is not legitimate.
- These scams can also take place over TEXT messaging. The fraudsters frequently use local presence dialing technology to mask their phone, and have it appear as if it is coming from someplace in the United States, when it is not.
- There is an insistence on urgency.

What should you do if you receive such an email or if an acquaintance forwards such an email to you?

Dos:

- Keep the original fraudulent message for further investigation
- Contact the Internet Service Provider (ISP) used to initiate contact and report the fraudulent activity.

Don'ts:

- Do not engage with original sender
- Do not deposit any checks
- Do not send or return any money to the original sender
- Do not forward the fraudulent email

By making you aware of these scams, we hope to keep you from being a victim of fraud, and ultimately to stop these scams.