Job Seeker Alert – Beware of Job Hunting Phishing Scams

Elkay was recently notified by several job seekers that they had been contacted by phishing scammers, masquerading as Elkay Recruiters.

We wanted to provide you with some guidelines to help you stay safe as you go about your job search.

What is a job hunting phishing scam?

Phishing is a crime committed by cyber thieves who are trying to obtain personal information such as home address, date of birth, social security and driver's license numbers, and bank accounts. Students and job seekers are often targets of these cyber thieves, because they post resumes (personal data) to conduct their job search online.

Emails are the most common form of contact for phishing scams. The thieves will pretend that they represent a legitimate company (such as Elkay) by using the company name in the body of the email.

Some common signs that you might have received a job hunting phishing scam

- The fake recruiter asks for personal information as described above
- The sender's email address comes from a "free" platform such as yahoo or gmail. (NOTE: Elkay's recruiters all have legitimate email addresses that end in @elkay.com)
- Email messages contain grammatical or spelling errors because many cyber criminals are based in other countries. The emails may include contaminated attachments that you have to open or download – these may harm your computer.
- The sender is offering you a job that pays higher than you would expect for work that seems easier than you might anticipate. The job is a "work from home" opportunity, and you are not asked to participate in an actual interview.
- The fake recruiter sends you a check, and asks you to send money back to them for "business expenses" related to your hire.

Here is how to protect yourself should you be contacted by a phishing scammer.

Be wary of unsolicited job offers. – Jot down contact information about the person offering the job as well as the job title. Check the email address against a bona fide email address that you might find on the company website. Reach out to the company and confirm whether that person is an actual employee, and determine whether the position being offered is legitimate. (Elkay jobs will all be listed on the corporate.elkay.com job search tool.)

Do not download files, click on hyperlinks, or deposit checks that might be sent to you. -- Files and links can be Trojan Horse files that can harm your computer. Cyber Thieves will rarely send you a legitimate check; unfortunately, by the time you find out the check is bad, you may have already sent money back to the thieves as they have requested.

Elkay will never offer you a job or send you a check prior to a formal in person interviewing and hiring process. Legitimate employers will never need money from a potential employee for submitting a resume or for processing background checks or credit reports.

Should you be contacted by someone that you suspect is a fake recruiter, always contact the company directly and confirm that the opportunity is legitimate. You can report phishing scams at the Federal Trade Commission (FTC.org) or the Anti Phishing Working Group (apwg.org).

We wish you the best of luck in your job search.
Check back at corporate.elkay.com often to see our current openings.

2222 Camden Court, Oak Brook, IL 60523 | (630) 574-8484 | elkay.com