Phishing Scam Alert

As an online job seeker, you could be a target of cyber (online) thieves seeking to secure personal information from you by sending you “phishing” messages.
Please be alert to and protect yourself from job phishing scams.
Read on to find out how you can avoid being a victim of job phishing scams.

1. What is a phishing/online job hunting scam?

Phishing is a common ploy used by cyber thieves to secure personal information such as home address, date of birth, social security/identification number and bank account numbers. Students and job seekers are often targets of cyber thieves.

Phishing emails are one of the most common forms of online scams. These emails are made to look like they are sent by a legitimate company or organization, including Santen, by forging the sender’s email address or using the name, logo and graphic of a legitimate company.

2. What are some signs of a job phishing scam?

- Sender’s email address assumes the appearance of a legitimate email address of a known organization or known email contact
- Email message addresses you generically, i.e., User, Customer, Client, Member or Sir/Madam
- Sender’s message may also include attachments that you have to open or download
- Sender requests that you respond to the email with your personal information

3. By doing the following you can help protect yourself from a job phishing or other online employment scam:

- Be wary of unsolicited offers of employment.

  Ascertain your source*. If you speak to someone over the phone about a job opportunity, ask questions and note information such as the name of the person, the company they represent, the location where they work, their office contact details and the opening they have. Go to the company website ‘contact us’ page and email or speak to someone from the company to verify your source.*

Phishing Scam Alert

- Always check the information provided in the email as it could be a phishing email.

  Verify sender's email address. *Emails tend to follow specific structures. Cyber thieves often use an email address or URL that looks legitimate. For example, instead of Santen.com, you may see Santen-co.com, Santen@yahoo.com, Santen-Inc@gmail.com or other variations. These are not legitimate addresses and are signs of a phishing scam.*

- Do not click on the hyperlink provided by sender whose email address you do not recognize.

  Check the legitimacy of the URL provided by the sender. *To access the company's actual website, research the prospective recruiter or employee's URL through a search engine.*

- Do not provide your personal data in response to an email.

  Do not share your personal data. *Do not email, fax or provide personal information over the phone. Personal information can include: bank account number, credit card number with security code, account user name and password, date of birth, driver's license number and full social security/identification number. Such information is typically requested by the hirer only at the end of a formal hiring process, i.e., after in-person interviews, an offer of employment, and the signing of an employment contract.*

- Beware of anyone who asks for your credit card number or check payment in order to pursue an opportunity.

  Do not transfer any money or send a personal check to pursue an employment opportunity *with Santen or any other company. Legitimate employers will never need money from a potential employee for submitting a resume or for processing background checks or credit reports.*

  If you are paying for job placement services, do not provide payment information through emails. When possible, payment for these services should be done onsite at the agency whose services are being used.

- Other red flags should be raised when:
  - Someone asks to conduct an interview over an "instant message" or "chat" connection
  - Emails from prospective employers contain typos and grammatical errors
  - Emails from prospective employer seek your response by offering 100% work-at-home jobs
  - You are offered a "job" without having had an in-person interview