December 8, 2017

Optoquest Co., Ltd.
President: Noboru Higashi

To whom it may concern,

Attention: Unauthorized use of company's email addresses by a third party

Our company's Internet provider reported us that someone sent out massive amount of spoofed emails using our employees' email addresses.

In order to prevent the occurrence of any damage caused by spreading spoofed emails, we report this matter accordingly. At the same time, we would like you to be careful about this issue.

[Current Status]

Immediately after we knew the incident, we asked our Internet provider to stop the email transmission from those addresses compulsorily. At the same time, we changed the passwords of those email addresses as well as all the employees' including relating staff members. No unauthorized use has been reported so far. However, in order to take a drastic measure, we're still investigating the matter.

[Request to All]

The email addresses used illegally were as below (2).

sudo_makoto096@optoquest.co.jp

takasaki@optoquest.co.jp

If ever you received any email from above addresses, delete it immediately without opening. If you opened the email by mistake, never access to the attached or URL in the message. If you could inform us of your receipt of such email, we'd really appreciate it so that we can investigate the problem further.

Contacts: Optoquest Co., Ltd. Business Dept., (Yamasaki or Sato)
Phne : +81-48-724-1811
E-mail : yamasaki_takaori033@optoquest.co.jp or sato-h@optoquest.co.jp

Sorry for this inconveniences caused and thank you very much for your understanding.

* Below is the detailed report of the occurrence of this incident and actions to take from now on.

Description of the incident (Unauthorized use of company's email address by a third party) and actions taken

1. Description of the incident

   On the 3rd December, 2017, our company's Internet provider detected that as many as 1482 emails, which number was abnormal, were sent out from sudo_makoto096@optoquest.co.jp and takasaki@optoquest.co.jp between 18:36 - 18:44 and 18:38 - 18:46. Therefore, we urgently asked our Internet provider to stop the email transmission from those 2 email addresses compulsorily. We identified that this suspicious email contains the URL in the body part; however, not any attachment.

2. Action taken

   We recognized the incident at around 9:00 (Business opening hour) in December 4. Then we took below actions.*

   ① Implemented a virus-check of the two employees' computers as well as all the company computers. No virus was detected.

   ② Changed the email passwords of the two employees as well as all the employees'.

   (* The incident happened on Sunday December 3 which was company holiday)

3. From now on

   Up until now, no further damage such as unauthorized access to our company server, an information leak, or data alteration was found; however, we will keep investigating this issue. If anything comes up, we'll take an adequate action accordingly. We will keep you inform the result. Also please be noted that some kind of information disclosure may be necessary if required.

   Although we have conducted the information control, the giving instruction as well as education on information security based on the company regulations, we will revise our operation and ensure even more effective management of the data.