

March 1, 2022  
SIGMAKOKI CO., LTD.  
Administrative Division

## **Beware of "Spoof Emails" Impersonating Our Employees**

We have been receiving an increasing number of reports from our customers and business contacts about spoofed e-mails sent in the name of our employees. We would like to inform you to be careful.

This is believed to be an attack e-mail targeting the spread of disruptions caused by a computer virus (malware) called "EMOTET".

In the e-mails sent by this malware, the real recipient's name, e-mail address, and part of the e-mail content are used to deceive, and the e-mails are very subtle, such as "pretending to be a reply to an official e-mail."

As for "spoof e-mails" with our employee's name as the sender's name, the e-mail address after the @ mark is not "sigma-koki.com".

Please delete such suspicious e-mails without opening them, or call the sender, who is our employee, or relevant section of our company to confirm if such e-mails have been sent.

Opening files attached to attack e-mails or viewing the URLs listed in the e-mails can cause disruptions from the virus, resulting in not only damage to your company, but also secondary damage such as unintentionally spreading the virus to others.

If you have any questions or information to provide, please contact the relevant section of our company.

Sincerely,