

September 3 2020

Dear Valued customers

Report on the spoofing mails caused by the malware called "Emotet".

Thank you for always supporting continuous business with Riken.

This is an urgent notice that our mail server has been attacked by unauthorized access.

We are truly sorry for this inconvenience caused, and we are investigating in this incident for the moment.

1. Summary of this fact:

We assume that the malware called "Emotet" has invaded our server and started to send targeted e-mail. This malware is characterized as below:1) Steal sender's outbox all histories2) Names, email addresses, part of email messages will be abused3) Send spoofing mail using stolen address randomly

2. How to handle:

When you find spoofing email, such as unfamiliar text with MS Word like attached file, please DO NOT OPEN NOR CLICK the attachment; then, please do delete them immediately.

3. Next action:

We are currently working on upgrading our security, such as improving firewalls to prevent the same incident again. As well, we will strengthen the management of personal data and recover trust.

We apologize again for causing you inconvenience, and we strongly hope you will not be hacked by this malware.

Riken Perfumery Co., Ltd.