Takatori Corporation

313-1 Shindo-cho, Kashihara-city
Nara, 634-8580 Japan

February 10, 2022

Subject: Emails pretending to be our employees

Dear Business Partners:

We would like to announce that we have confirmed the fact that suspicious emails disguised as our employees are being sent to multiple people.
We are currently conducting a detailed investigation into this matter with the cooperation of the local police.
There will be a risk of computer virus infection or unauthorized access by opening the file attached to the suspicious email.
If you receive a suspicious email, please refer to the following identification method and DELETE the entire email without opening the attached file.

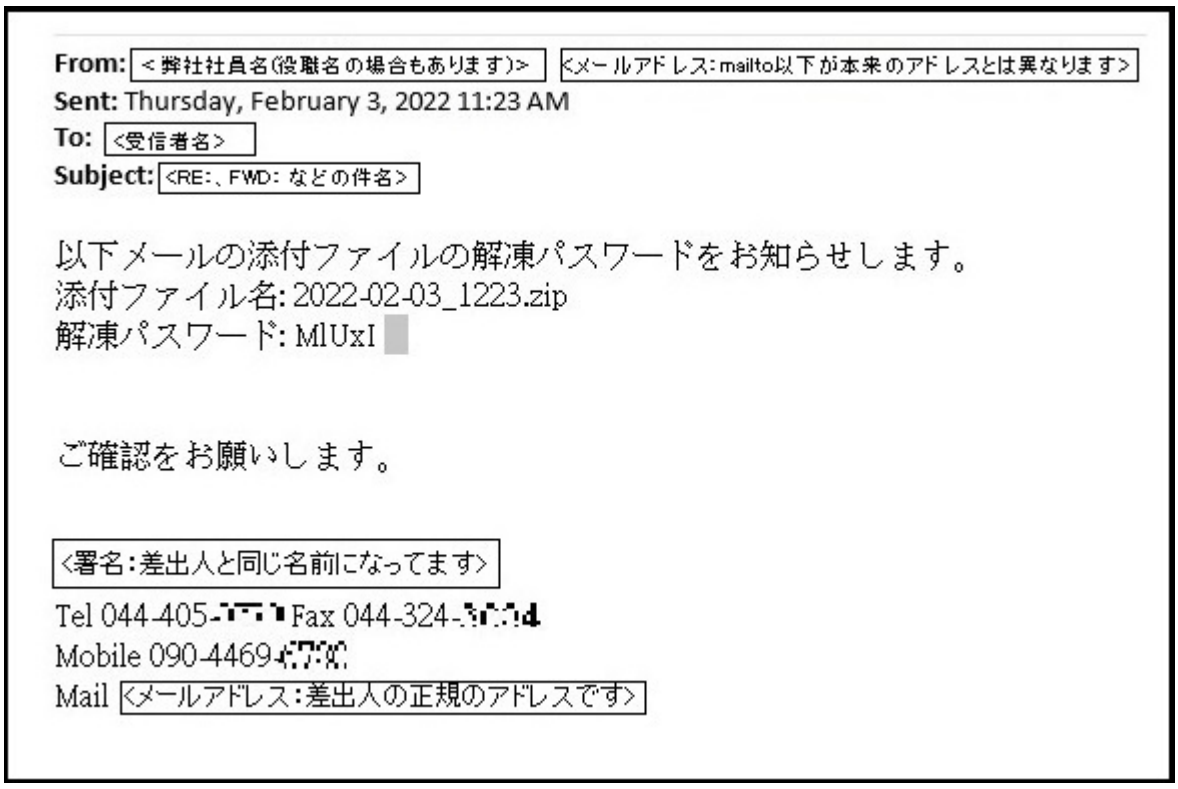
If you accidentally unzip the ZIP file or open the Excel file, please disconnect the network immediately and scan all drives with anti-virus software.
Also, depending on the version of the anti-virus software, it may not be possible to detect or quarantine the virus, so it is recommended to initialize the PC.
*It is recommended to initialize the PC if anti-virus software is not installed.

[How to identify suspicious emails]
The suspicious emails confirmed are as follows:

- The sender (from :) is displayed as our employee's name, but the email address is different.

- If the domain of the email sender is takatori-g.co.jp, it is a legitimate email from our company.
- As for the attached file, .xls and .zip have been confirmed.
- In many cases, the subject (subject :) is the recipient's name.
- There may exist other patterns that are not listed above.

An example of suspicious email (the email is written in Japanese)：



*The displayed contents will differ depending on the mail software.

We apologize for the inconvenience. If it is difficult to determine whether the email is suspicious, please contact our employees.

Sincerely,