January 29, 2025

To whom it may concern:

NOF CORPORATION

Beware of Scam Emails and Phone Calls Impersonating NOF

1. Receiving emails from imitation domain names that seem to belong to NOF

We confirmed that emails had been sent in July 2023 impersonating a NOF officer.

In this case, the emails had been sent from domain names that imitated ours. The sender pretended to be a NOF officer who demanded that the recipients provide personal information and transfer money.

Please confirm that emails sent to you that appear to be from NOF include our correct domain name, @nof.co.jp. Please also pay close attention to the content of emails for anything that seems suspicious.

Examples of domains that were used:

"@nofcorporation.com"

"@nof-corporation.com"

2. Receiving emails impersonating a legitimate domain name

We confirmed that an email had been sent in April 2024 impersonating a NOF officer.

In this case, the sender information of an email had been changed to make it look like it came from a legitimate domain name. The sender pretended to be a NOF officer, urging the recipient to contact him later.

As a security measure, NOF has introduced email authentication technology called DMARC*. DMARC verifies that senders are legitimate, preventing the sending of spoofed emails impersonating NOF personnel.

The domain name in question is "@nof.co.jp."

* DMARC stands for **D**omain-based **M**essage **A**uthentication **R**eporting and **C**onformance.

3. Receiving scam phone calls impersonating NOF officers

We have confirmed that people impersonating NOF officers have been making scam phone calls. They attempted to do things such as obtain information on your accounting personnel. Please also pay close attention during phone calls for anything that seems suspicious.

If you have any questions about the above, please contact:

Corporate Communications Dept.
NOF CORPORATION
Email: info@nof.co.jp