NOF CORPORATION

June 17, 2024

To whom it may concern

Beware of Fraudulent E-mails Deceiving Our Company

1． Receiving mail from a similar domain

In July 2023, it has come to our attention that some persons have received emails masquerading as being sent by a NOF CORPORATION officer.

In this case, emails were sent from a domain similar to ours, impersonating our company's officer and requesting personal information and remittance.

Please confirm that the sender's email address is our domain “…@nof.co.jp” and pay careful attention to any suspicious features in emails.

Example Domain of fraudulent emails

「・・・@nofcorporation.com」

「・・・@nof-corporation.com」

2． Receiving mail pretending to be a legitimated NOF’s domain

In April 2024, it has come to our attention that one person have received an email impersonating NOF CORPORATION officer.

In this case, it was an "impersonating email" that deceiving NOF’s legitimated domain and sent a message pretending to be our company’s officer and urging further communications.

We have introduced an email authentication technology called "DMARC".

DMARC is an email authentication technology that verifies the authenticity of the sender, and prevents "impersonating email" that deceiving our company.

Applicable email domains is “@nof.co.jp”.

DMARC：Domain-based Message Authentication Reporting and Conformance

Contact

Corporate Communications Dept.
NOF Corporation
Tel: +81-3-5424-6600　E-Mail:info@nof.co.jp