“Szanowni Państwo,

W dniu 17 stycznia 2022 otrzymaliśmy informację o próbach infekowania złośliwym oprogramowaniem przy pomocy maili podszywających się pod komunikację od BNP Paribas Leasing Services Sp. z o.o..

Jak rozpoznać fałszywą wiadomość:

1. Nie pochodzi z żadnego z poniższych adresów:
   - do_not_replay@corp.bnpparibas.com
   - windykacja.leasing@corp.bnpparibas.com
   - statusy-noreplay@bnpparibas.com
   - efakturybplg.leasing@bnpparibas.com
   - statusy-noreplay@corp.bnpparibas.com
   - noreply_leasing@corp.bnpparibas.com
   - do_not_replay@bnpparibas.com
   - do_not_replay@bnpparibas.com
   - job_fol@corp.bnpparibas.com
   - ksiegowosc.leasing@bnpparibas.com
   - statusy.leasing@bnpparibas.com
   - windykacja.leasing@bnpparibas.com
   - efaktury.bnpls.leasing@bnpparibas.com
   - bpm-notification@corp.bnpparibas.com
2. Zawiera załącznik w postaci zaszyfrowanego hasłem pliku .zip
3. Hasło do pliku .zip podane jest w treści maila

Dla Państwa bezpieczeństwa bardzo prosimy o nieotwieranie załącznika i usunięcie wiadomości z Państwa poczty elektronicznej.

Chcemy stanowczo stwierdzić, że BNP Paribas Leasing Services Sp. z o.o. nie jest źródłem tej komunikacji i będzie aktywnie współpracować ze wszystkimi instytucjami w celu ustalenia i ukarania osób rozsyłających fałszywe i szkodliwe wiadomości.”