Email Spoofing

Dear Client,

We would like to remind you that Email spoofing is a technique cyber attackers **use to conceal the sender's realaddress,** malicious links or malware under a forged address —**usually an apparently legitimate address— in order to assume the identity of a company**, institution, or someone you know.

Therefore, we recommend the following::

- Do not open suspicious emails or emails from people you don't know. **Do not click on links** or open documents attached in mails from people you don't know.
- Verify any **changes to the sender's usual address.** If you are unsure about an email from Monex, contact your Monex Executive to confirm the authenticity of the message.
- Pay attention to **unusual writing,** such as misspellings and attempts to convey a sense of urgency.
- **Get a managed service** and enable sender identity verification protocols (SPF, DKIM, DMARC).
- Use security tools, such as an anti-spam filter.
- Verify your antivirus and malware protection systems are up-to-date.

Should you have any questions about suspicions emails from Monex, please contact your Monex Executive or call at 55 5231 4500 in Mexico City, or 800 746 6639 elsewhere in Mexico.

MONEX

Saty agile

monex.com.mx