ATTACK ON YOUR INBOX:

E-MAIL SPOOFING

HOW DOES E-MAIL SPOOFING BECOME A TRAP?

- Fraudsters track internal or intercompany e-mail traffic or replicate previously compromised email threads to send fraudulent messages primarily to accounting and finance departments. The sender addresses are subtly altered to appear legitimate, often by replacing the lowercase letter "l" with an uppercase "I" or the letter "o" with the number "0," making visual detection extremely difficult.

- These fraudulent emails often contain phrases such as "*Our bank account details have been updated.*" or "*Urgent payment is required.*" To make the content appear convincing, excerpts from real email threads, company-branded signatures, and attachments are commonly used. The ultimate goal is to divert high-value payments to bank accounts controlled by the fraudsters.

- This method, which involves infiltrating a target company's routine financial processes and exploiting security vulnerabilities, is particularly common among multinational corporations, large supply chain networks, and organizations with high volume email communications. It can lead to significant financial losses.

LEGAL ASSESSMENT

- **Article 158 of the Turkish Commercial Code ("TCC"):** The relevant act may constitute the offense of aggravated fraud, as it is committed through information systems.
- ***TCC Articles 243–244*:** Unauthorized access to email systems and actions such as data manipulation may be classified as cybercrimes under these provisions.
- ***TCC Article 282*:** The transfer or integration of funds obtained through this method into the financial system may constitute the offense of laundering of assets derived from criminal activity (money laundering).

HOW PREPARED IS YOUR COMPANY?

- Email security settings such as SPF, DKIM, and DMARC must be properly enabled on corporate email systems. These protocols help prevent fraudulent emails from being sent on behalf of the company.
- High-value payments must always be subject to dual control. Payment instructions should be verified not only through internal systems but also *via* direct phone confirmation.
- Accounting and finance teams should be regularly informed and trained on email fraud schemes. In particular, **awareness should be raised among employees to carefully check email domains and refrain from clicking on suspicious links when encountering potentially fraudulent emails.**

VARDAR ŞANLI IN ACTION:

- We meticulously manage all criminal proceedings related to fraud cases involving e-mail spoofing.
- As part of compensation for damages, we determine the liability of third parties, including banks and payment institutions acting as intermediaries and initiate the necessary legal processes.
- We also develop action plans outlining legal and operational measures against suspicious transactions and organize awareness trainings to mitigate future risks.

ATTACK ON YOUR INBOX:

E-MAIL SPOOFING

From: mkaya@ericgesssen.com
Sent: Monday, June 23, 2025 6:32 PM
To: Ahmet Yılmaz <ahmet.yilmaz@suppliercompany.com>
Subject: Fw: Payment Instruction for Invoice No: WL-1234 - ASAP

Dear Ahmet,

Please be informed that the bank account details for the payment of the previously sent invoice have been updated. The revised invoice is attached herewith. We kindly ask you to urgently process the payment of USD 900,000.00 to the account of our Italian subsidiary, the details of which are provided below.

Invoice No: WL-1234
Amount: USD 900,000.00

Account Name: **Eric Gessen Italia Limited**
Account Number: 123456
IBAN: TR 25000001234567891230123
Currency: USD

Thank you,

Mehmet Kaya
Finance Director
Eric Gessen Global Holdings Ltd.

From: mkaya@ericgessen.com
Sent: Monday, June 23, 2025 2:21 PM
To: Ahmet Yılmaz <ahmet.yilmaz@suppliercompany.com>
Subject: Payment Instruction for Invoice No: WL-1234

Dear Ahmet,

We kindly request your support in ensuring that the payment for the invoice detailed below is processed within this week.

Invoice No: WL-1234
Amount: 900.000,00 USD

Account Name: **Eric Gessen Global Holdings Limited**
Account Number: 123456
IBAN: TR 25000001234567891230123
Currency: USD

Thank you,

Mehmet Kaya
Finance Director
Eric Gessen Global Holdings Ltd.