Habib Bank AG Zurich
(Incorporated in Switzerland 1967)

Email Payment Fraud

What it is and how to avoid it

1) What is an email payment fraud?

Email payment fraud, also known as email invoice fraud or business email compromise (BEC), is a type of scam where fraudsters impersonate a legitimate business or individual through email communication to deceive victims into making payments or transferring funds to fraudulent accounts.

2) Here's how it typically works

Impersonation: The fraudster gains access to or spoofs the email account of a legitimate business or individual. They may also create an email address that closely resembles that of a legitimate entity.

Social Engineering: The fraudster then sends emails to targeted individuals, such as employees of the targeted business or its clients, suppliers, or partners. These emails often appear urgent and may request payments for invoices, bills, or services.

False Information: The email may contain fraudulent invoices, payment instructions, or requests to update payment details. Sometimes, the fraudster may even pose as a senior executive within the company, instructing employees to make payments urgently.

Redirecting Payments: The fraudulent emails typically include instructions to transfer funds to a bank account controlled by the scammer. This account is often set up specifically for the purpose of receiving fraudulent payments.

3) Who is responsible for the loss in an email Payment Fraud?

In cases where an individuals and businesses fall victim to email payment fraud and initiates the unauthorized transfer of funds, they bear responsibility for the loss.

4) How can you protect yourself from an email payment fraud?

Protecting yourself from email payment fraud requires a combination of awareness, vigilance, and implementing security measures. Here are some steps you can take to reduce the risk:

Verify Requests: Always verify payment requests, especially if they come via email. Use alternative communication channels, such as phone calls or in-person conversations, to confirm the authenticity of the request with the sender.

Double-Check Details: Carefully review all payment instructions, invoices, and email addresses for any discrepancies or irregularities. Check for spelling mistakes, unusual formatting, or changes in payment details.

Train Employees: Educate employees about the dangers of email scams and the importance of verifying payment requests. Provide training on how to recognize phishing emails and fraudulent payment requests.

Establish Procedures: Implement clear procedures for verifying and authorizing payments. Require multiple layers of approval for large transactions, and ensure that sensitive financial information is only shared on a need-to-know basis.

Implement Email Security Measures: Deploy email security solutions, such as spam filters, antivirus software, and email authentication protocols to detect and prevent email spoofing and phishing attempts.

Be Skeptical of Urgency: Be cautious of emails that create a sense of urgency or pressure you to act quickly.

50 YEARS IN UAE
Habib Bank AG Zurich