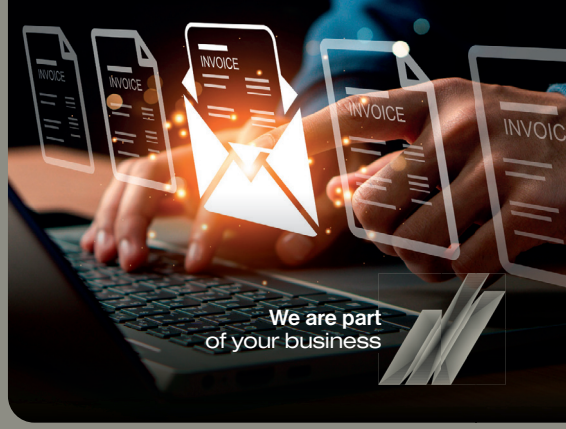
How to Avoid **Invoice Payment Fraud**



Invoice fraud is a scheme in which an attacker attempts to extract money from a company through fake or altered invoices while posing as a legitimate supplier. Common scenarios include:

Business Email Compromise

The attacker gains access to email correspondence through manipulation or phishing and inserts themselves into the conversation between the company and its business partner.

Fake Invoices

The attacker generates an invoice that looks identical to one from a real vendor (with only the email address or bank account number changed) and sends it to the company, seeking payment for goods or services that do not exist.

Altered Payment Details

The attacker alerts the company to an upcoming “change” in bank account information, providing new details so that future payments are diverted to an account the fraudster controls.

How the Attacker Communicates

The fraudulent invoice is virtually **indistinguishable from the genuine one** (same logo, address, company ID), except for **the payment details** (IBAN). This change is easy to overlook. The attacker relies on the assumption that the employee will not verify the accuracy of the data, given the long-standing business relationship, and may apply **pressure tactics**, such as emphasizing overdue payments or insisting the new account information be used immediately. Always verify any change in payment instructions through a **separate contact channel, not simply by replying to the original email**. In practice, the attacker may pose as either a current or a new business partner.

Invoice fraud can have severe, even catastrophic, financial consequences. Minimizing the risk requires robust internal controls:

1. Change Safeguards

Establish a formal **approval process for any modifications** to invoicing or payment data.

2. Supplier Verification

Rigorously confirm a **supplier’s identity** and bank details before processing payments.

3. Internal Trainings

Educate employees about fraud risks so they can spot suspicious behavior.

4. Two-Factor Authentication

Require **two-factor authentication** for access to sensitive systems and information.

5. Regular Audits

Periodically review processes and systems to **uncover potential weaknesses**.

Real Situations Where You Might Encounter Fraudulent Invoices

Existing Business Partner:

1. A fitting example is a multinational property-management company with a Slovak subsidiary (Limited Liability Company) that is coordinating an intercompany loan repayment with its parent company.
2. However, **the email chain**, conducted in technical legal and financial language between a lawyer representing the parent company and the Slovak employee in charge of loans, is **compromised**.
3. **The attacker alters the original email address** by swapping two visually similar letters.
4. A document is sent instructing the subsidiary to repay the loan to a Polish bank **account that actually belongs to the attacker**.

Routine correspondence with the existing supplier

Email account compromised

Fraudulent invoice sent from a subtly modified email address

New Business Partner:

1. A customer wants to purchase a piece of technology and follows the usual buying process. They locate the supplier's website and initiate contact (first time dealing with the company).
2. The customer receives and pays an invoice, but the goods never arrive.
3. Upon contacting the supplier through different channels, they learn **the website had been hacked** and the company never carried such inventory.
4. A situation may also arise where the website itself is legitimate, but **an attacker infiltrates the genuine supplier's email** just after the customer places an order.
5. The attacker's fraudulent invoice is **sent to the customer for payment**.

Contacting a new supplier and ordering goods

Website may be hacked, leading to a fake invoice

Email correspondence may also be hijacked, leading to a fake invoice

TATRA BANKA
Member of RBI Group