paymerang | finance automation for the modern enterprise

SEVENTY-FOUR PERCENT OF ORGANIZATIONS WERE TARGETS OF PAYMENT FRAUD IN 2020

Here are 3 types of fraud to look out for:

BUSINESS EMAIL COMPROMISE

BEC is when scam artists use emails to dupe accounting departments into transferring funds into illegitimate accounts.

BUSINESS EMAIL COMPROMISE
EXAMPLE

A company ceo asks an employee to purchase gift cards to send out as employee rewards. He asks for the serial numbers so he can email them out right away.

VENDOR IMPERSONATION

Fraudsters send fake emails to companies asking for payment.

VENDOR IMPERSONATION
EXAMPLE

A fraudster might use **john.kelly@compony.com** (an extra **"O"** in company) instead of **john.kelly@company.com** to trick victims into thinking their email is legitimate.

PHISHING

Fraudsters send a fake message designed to trick a human victim into revealing sensitive information so the attacker can expose the victims device to malicious software, get their credit card info and passwords.

PHISHING
EXAMPLE

You receive an email with a link to confirm your payment information. The sender is warning you that your account is suspended until you take time to verify your account information.

It's imperative that businesses conduct quarterly trainings to educate their team on fraud prevention. All it takes is one bad click for an entire organization to crumble.