Allianz

Allianz Trade

HOW TO PREVENT FAKE-BUYER FRAUD AND PAYMENT DIVERSION?

How to protect against Social Engineering?

More refined methods by external criminals require increased attention at all corporate levels. Fortifying your first line of corporate defense is key to successful threat mitigation.

Defending not as easy as it once was

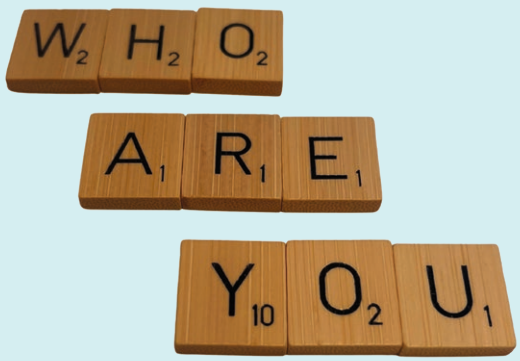
Fake-Buyer Fraud, also known as Fake-Identity Fraud has seen consistent double-digit growth rates over years on end. While fraudsters previously used simple false ID to pretend to be a buyer and withdraw with the goods and services received before paying, today's schemes are far more sophisticated. In contemporary methods, entire shell-corporations and call-centers with credible cross-referencing between forged documentation and multiple dialogue partners are the norm. These efforts make the fraud very hard to detect for an untrained eye.

Cash-flows at risk

Incidents involving external criminals diverting payment streams are on the rise as well. Fraudsters target a specific employee while impersonating business partners and create fictious invoices or other instructions to divert payments to criminal-controlled bank accounts. While less frequent than Fake-Buyer Fraud, it tends to impact cash-flows even harder, as amounts transferred are typically significant because the discovery takes time.

Success factors for risk mitigation

1. Active risk governance with **KPIs**
2. Iterative adjustment of **corporate guidelines**
3. Continuous internal **awareness trainings**
4. Effective risk mitigation with **dedicated software** products or insurance solutions



Three-Factor-Authentication

Note that any two factor authentication is insufficient in today's environment as the fraudster will likely have forged at least one factor, i.e. the instruction letter, fake-voice call, etc.

Establish third factor authentication for business processes at risk, for example:

- Bank account changes
- Supplier change
- Entering any login credentials

The third verification source can be a validation of the newly presented source with physical or historic evidence, i.e. calling the business partner under existing known number or asking a colleague for a cross-check.

+ 400 %
Social engineering fraud cases have increased fivefold since 2014

+ 18 %
Increase in social engineering fraud cases 2022 vs. 2021 alone

Source: Allianz Trade loss statistics

Consider the human vulnerability in order to avoid it
External perpetrators exploit the weakest link – the "human vulnerability" of employees by manipulating them. Today a mix of social engineering techniques is state of the art. And although these scams are not new, and even though many companies are sensitizing their employees, the number of cases continues to rise.

Engagement key for prevention
With technological progress Social Engineering attempts are expected to not be obvious at first glance anymore. Taking a commonly known form of Social Engineering as example, emails with forged instructions will soon not contain any typos or grammar mistakes anymore, as generative AI's are perfectly capable of eliminating these during the creation process.

One way to address this is to actively engage and incentivize constructive thinking and thereby reminding everyone to keep an alert and vigilant stance. This is a lowthreshold type of measure – the challenge is to act at once and start continuous internal awareness training.

Exposure increased over 400 % in less than a decade
Claims levels five times over the level recorded not even ten years ago require counter measures to offset the elevated crime-levels.

Next to internal awareness training, iterative adjustment of corporate guidelines and active risk governance, modern software solutions can improve security. They support and automatize black-listing domains, email-patterns or proactively blocking bank accounts used by criminals.

A residual risk always remains
Even with perfect risk mitigation infrastructure, one inattentive moment, just one overworked colleague or simply a perfect fraud scheme can be enough for a profit warning to be issued.

From a modern risk management perspective the question is not if, but when your corporation is hit. Research shows organizations around the world lose significant portions of their annual revenues to internal and external fraud. Exact figures differ depending on type of analysis, yet some sources state ca. 5 % – on average.

Allianz Trade offers solutions to protect your company against financial losses through willful unlawful acts by insured persons and certain third parties.

Any questions for us? Whether you are already a customer or not, we will be delighted to help.

+41 848 544 544
fidelity.ch@allianz-trade.com
www.allianz-trade.ch

Ten common signs of Fraudulent Emails:

1. Missing or unusual salutation
2. Unfamiliar tone
3. The message creates a sense of urgency
4. It includes suspicious attachments or links
5. Request for credentials, payment information or personal details
6. Inconsistencies in email addresses, link and domain names
7. The message is sent from a public instead of a business email domain
8. Content, e.g. product offer is too good to be true
9. Email written in foreign language
10. Recipient didn´t initiate the conversation

Euler Hermes Switzerland
Office Lausanne
Office Lugano

Richtiplatz 1
Chemin de Bérée 52B
Via Guido Calgari 3

8304 Wallisellen
1010 Lausanne
6900 Lugano

fidelity.ch@allianz-trade.com
www.allianz-trade.ch
T +41 848 544 544