COMBATING RISING FRAUD WITH ENHANCED PAYMENT SECURITY

With the rise of digital transactions, fraudsters are intensifying their focus on companies, thereby triggering a notable rise in payment fraud. According to PwC's Global Economic Crime and Fraud Survey 2022, 51% of businesses worldwide have suffered some form of fraud within the last two years. This marks the highest incidence of fraud recorded in the past two decades. Fraudsters have intensified their attacks, they strike more often and are not afraid to go after large companies. To avoid falling victim to payment fraud, how can you secure your banking procedures and payment processes?

WHY ARE FRAUD ATTEMPTS ON THE RISE?

Fraudsters are no longer afraid to target large companies, focusing their efforts where they can divert large amounts of money. 25% of companies that were victims of fraud reported losses exceeding $1 million, as per the PwC survey. Companies without a payment management platform are also more vulnerable. "You have to connect to the website of each bank to make payments. The authentication and validation procedures for payments are not homogeneous, and the bank information is present on several websites", explains Stéphanie Bombart, Executive Director at Exalog, editor of Allmybanks software. Moreover, many companies host their software internally, which increases risk exposure. Fraud is becoming more sophisticated and fraudsters more professional. To fight against their new advanced digital technologies, opting for a specialized software editor will guarantee maximum data security. Procedures are also more and more digitized but employees are insufficiently informed and trained about risks of fraud, as Stéphanie Bombart says: "Another risky situation is when processes are heavily digitized without regular user training and awareness of fraud risks".

BE AWARE OF CYBERCRIMINALS' TECHNIQUES

To prevent fraud, start by recognizing it. Among the most used techniques, the top three favored by cybercriminals are:

- Fake supplier fraud,
- Fake president fraud,
- System intrusion.

In the first two instances, cybercriminals impersonate a familiar person in order to gain the trust of their interlocutor. Companies have also observed an increase in phishing attempts, a technique designed to trick victims into divulging personal data, such as banking credentials, and passwords.

BEST PRACTICES TO PREVENT FRAUD ATTEMPTS AND SECURE YOUR PAYMENTS

In light of the growing sophistication of fraud tactics, it is essential to implement and regularly update best security practices.

A payment management software can secure your payments and guarantee security for both payment procedures and data. "A software editor specialized in financial flows will handle the infrastructure, data backups, and ensure maximum security", explains Stéphanie Bombart. The payment management platform will allow you to implement task segregation to designate who is authorized to perform various tasks in the payment chain: "A single person should not be able to carry out all the steps of the payment in the application", advises Dominique Coste, Sales Director at Exalog.

A payment software will also allow you to set up validation workflows on payments, to modify your suppliers' banking information securely, and to add a white list of countries for your payments.

Opting for the automation of flows between your payment management software and your other management software (ERP, accounting software) will minimize human intervention and associated error and fraud risks.

HOW TO CHOOSE YOUR PAYMENT SOFTWARE?

When choosing a payment management platform, it is important to ensure its sontinual evolution to comply with the best security practices.

Make sure you can manage user authorizations so you can easily implement task segregation and update rights as your organization grows. This will allow you to better manage security. Avoid per-user contracts so you can remove and add users as you wish without additional cost. Choose a SaaS solution, which will be synonymous with agility, ease of use, and deployment.

"Our Allmybanks software, designed for groups with subsidiaries, is based on these very parameters," confirms Stéphanie Bombart.

MORE INFORMATION ABOUT payment security, you can download this white paper: https://www.allmybanks.com/en/white-paper-payment-security

Dominique Coste, Exalog

Stéphanie Bombart, Exalog

© DR