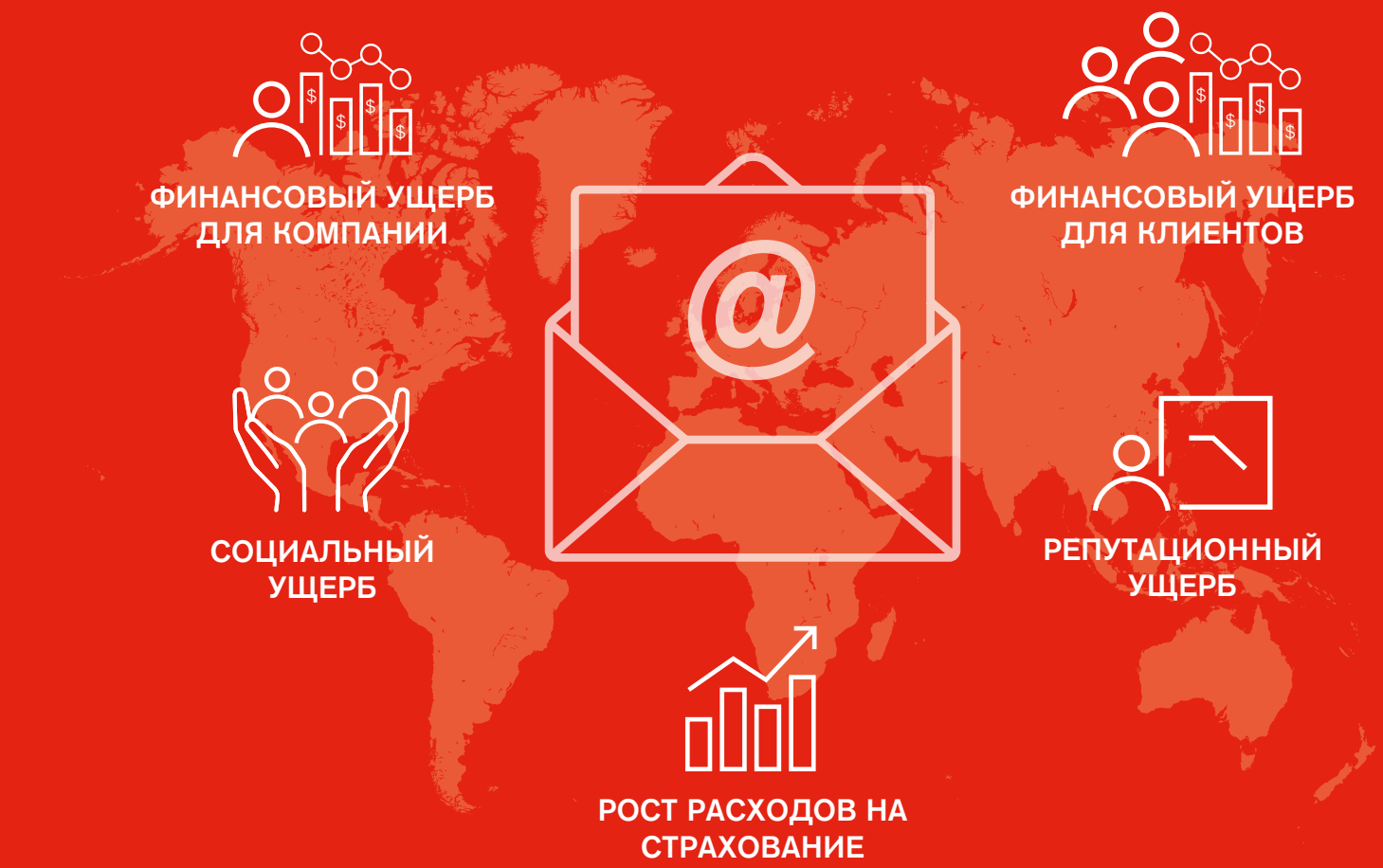
Мошенничество: риски при работе с электронной почтой

Знаете ли вы, на что обращать внимание?

Если вы работаете в международной цепочке поставок, ваша деятельность может стать целью для мошенников, которые разными способами внедряются в корпоративную систему электронных платежей. Такими махинациями обычно занимается организованная группа, участники которой находятся в разных точках мира, а похищенные средства могут идти в криминальный сектор, связанный с терроризмом, контрабандой наркотиков, торговлей людьми.

Сегодня коммуникации и финансовые транзакции повсеместно осуществляются в онлайн-режиме, поэтому риски мошенничества, связанные с использованием электронной почты, существенно возросли и требуют предельной бдительности и дополнительных проверок. В данной памятке мы покажем наиболее распространённые способы мошенничества с электронными платежами и меры, которые помогут компаниям снизить риски.

С какими рисками вы можете столкнуться?



Какие способы мошенничества с платежами встречаются чаще всего?

ПОДЛОЖНЫЕ ЗАПРОСЫ НА ПЛАТЁЖ

Чаще всего мошенники выдают себя за вашего знакомого контрагента, которому вы регулярно переводите платежи, но просят произвести очередной платёж на другой счет. Мошенники мониторят электронную почту в ожидании подходящего запроса на оплату, копируют стиль и язык сообщения, чтобы не вызвать подозрений. Часто адрес электронной почты, который они используют, сложно сразу отличить от адреса корреспондента, с которым вы обычно ведёте переписку.

ПОДДЕЛКА РАСПОРЯЖЕНИЙ РУКОВОДСТВА

Распространённым видом мошенничества с платежами является отправка по внутренней электронной почте фейкового письма от лица генерального директора или иного уполномоченного сотрудника с требованием произвести платёж новому контрагенту/клиенту или оплатить счёт, который похож на счета существующего клиента.

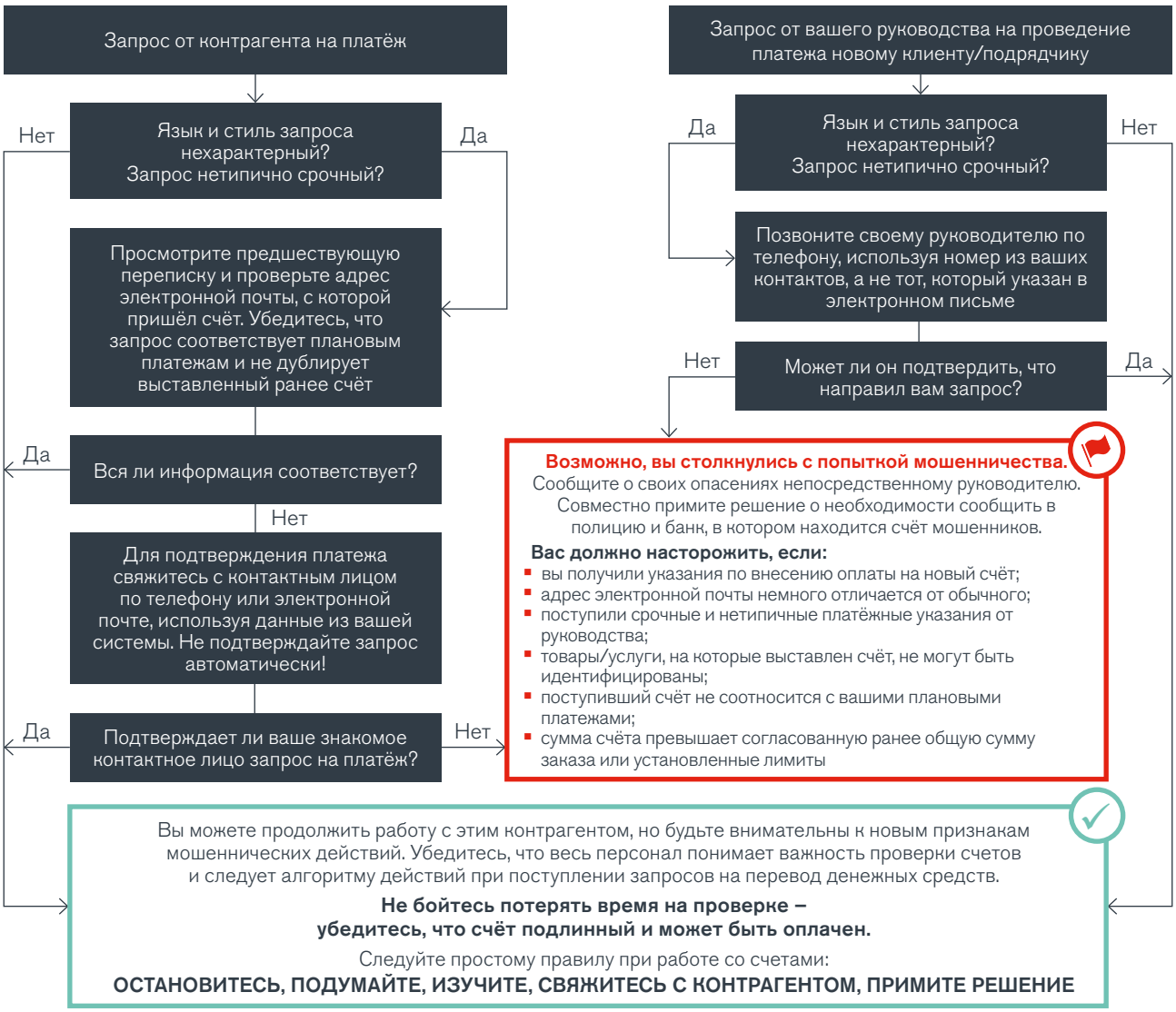
МОШЕННИЧЕСТВО ОТ ЛИЦА СУБПОДРЯДЧИКОВ

Работа в глобальной цепочке поставок обычно требует привлечения различных субподрядчиков, что повышает риск мошенничества с поддельными счетами за оказанные услуги.

Мошенники могут взломать вашу корпоративную систему и отследить электронную переписку, чтобы собрать необходимую информацию и выставить поддельный счёт. Часто его трудно сопоставить с конкретной услугой, или он может копировать предыдущий заказ, но с другими банковскими реквизитами.

Мошенники также могут использовать различные приёмы давления, чтобы ускорить проведение платежа без дополнительных проверок: указывать на негативное влияние задержки на кредитный рейтинг, статус и репутацию компании или угрожать судебным преследованием в случае неуплаты по выставленному счёту.

Чтобы не стать жертвой мошенников, при работе с электронной почтой следуйте алгоритму проверки:



TT CLUB
IS MANAGED
BY **THOMAS MILLER**

За дополнительной информацией
обращайтесь на **ttinfo@panditrans.com**
и заходите на **www.ttclub.com** и **www.panditrans.com**