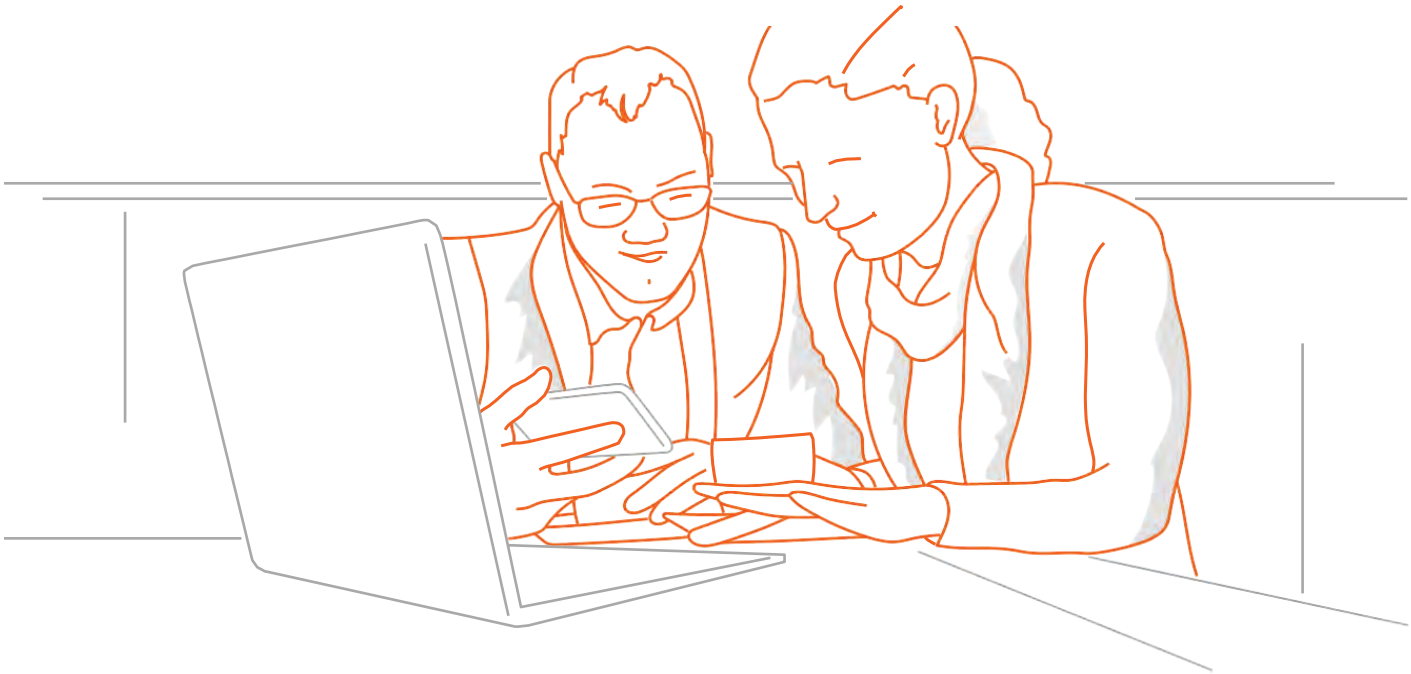
Что делать в случае мошенничества?



Если Вы подозреваете, что происходит мошенничество, незамедлительно сообщите об этом Вашему клиентскому менеджеру или в службу технической поддержки Банк-Клиента. Несмотря на то, что платежи обрабатываются и отправляются в режиме онлайн, ИНГ сделает все возможное чтобы приостановить неправомерное списание денежных средств с Вашего счета. Помните, что скорость важна, потому что шансы приостановить платеж уменьшаются с каждой минутой.

Часы работы ИНГ:
С понедельника по пятницу: с 9:00 до 17:30

Контакты технической поддержки:
т.: +7 499 951 2567
e: InsideBusiness.Support@ing.com

Что делать в случае сомнения?

Лучше перестраховаться, чем потом пожалеть: О любом подозрительном платеже, нестандартном/неузноваемом интерфейсе Банк-Клиента, сомнительном сообщении следует уведомить ИНГ.

Что если ИНГ обнаружит подозрительную активность?

Если ИНГ заметит подозрительную активность, например сомнительные (неудачные) попытки входа в Банк-Клиент или нетипичные платежи, представитель Банка свяжется с Вами для дополнительного подтверждения проведения отправленных платежей. Если у Вас появятся сомнения относительно личности звонящего, Вы всегда можете сообщить об этом вашему клиентскому менеджеру

Что вам необходимо сделать

Если Вы стали жертвой мошенничества, вам необходимо обратиться в правоохранительные органы. ИНГ не может за Вас это сделать, но может посоветовать шаги, которые необходимо предпринять.

В случае мошенничества, например, мошенничества со счетами, мошенничества с помощью приемов социальной инженерии или мошенничества от имени должностного лица, мы настоятельно рекомендуем перепроверить остальные платежи на предмет их правомерности, т. к. зачастую мошенники в случае удачной первой попытки продолжают попытки незаконного списания денежных средств со счета жертвы.

Защитите себя от мошенничества

Узнайте о наиболее частых случаях мошенничества, которые могут повлиять на бизнес, и ознакомьтесь с рекомендациями по защите от них.

Мошенники умны, хорошо организованы и мастерски владеют приемами социальной инженерии. Они используют обман, чтобы манипулировать людьми для совершения действий или разглашения конфиденциальной или личной информации, используемой для мошеннической деятельности.

Случаи мошенничества, которые описаны ниже, не тривиальны, они происходят ежедневно во всем мире и приносят миллионы убытков. Будьте осторожны.

Наша роль

В случае мошенничества мы будем выступать в качестве посредника между Вами и банком-получателем. Мы сообщаем банку-получателю, что платеж был совершен в результате мошеннических действий, и просим приостановить зачисление денежных средств или вернуть их обратно. После получения сообщения от нас банк-получатель проводит расследование и решает, какие действия могут быть предприняты с платежом в соответствии с действующим законодательством.

Мы, со своей стороны проводим дополнительные проверки, чтобы выявить подозрительную активность на Ваших счетах. Обращаем Ваше внимание, что если платеж проводится в рамках стандартной активности, он будет рассмотрен как регулярный платеж компании.

Как использовать эту памятку?

Распространите ее в своей компании, чтобы повысить осведомленность сотрудников, особенно сотрудников, которым разрешен доступ к расчетным счетам Вашей компании или которые могут создавать и/или подписывать платежи. Мошенники часто нацелены на сотрудников с такими правами и полномочиями.

Несмотря на то, что нет полной защиты от киберпреступности, осведомленность может помочь распознать ее признаки!

Следуйте рекомендациям в работе, чтобы снизить риск мошенничества!

Мошенничество в сфере электронного банкинга, что это?

Мошенничество в сфере электронного банкинга подразумевает под собой фишинг и вредоносные программы. Оно может затронуть работу компании и Вашу личную жизнь. В любом случае, киберпреступники будут пытаться украсть деньги, используя украденные логин, пароль и электронные подписи.

Что происходит?

1. Представьте, что Вы получаете электронное письмо из Вашего банка, в котором говорится, что банк выполняет проверку безопасности/ваш счет будет заблокирован/банк меняет некоторые из своих услуг. Цель письма - заставить вас перейти по ссылке, указанной в сообщении, которая перенаправит вас на ложную страницу мошенника, похожую на вход в Банк-Клиент.
2. Перейдя по этой ссылке, Вы вводите свой логин и пароль, для входа в Банк-Клиент, тем самым раскрывая их мошеннику для отправки платежа от вашего имени с вашего счета..

Варианты такого мошенничества

- Вам звонит мошенник и представляется сотрудником банка. Он просит Вас войти в систему для проверки безопасности или обновления данных, а после этого продиктовать ему Ваш логин и пароль. Мошенник воспользуется полученными данными для доступа в Банк-Клиент и подписания платежа от Вашего имени.
- Ваш компьютер заражен вредоносным программным обеспечением. Обычно это происходит в результате перехода по ссылкам или открытия документов, прикрепленных к вредоносному сообщению, а также при посещении скомпрометированных веб-сайтов, которые используют уязвимости в Вашем браузере или операционной системе.

В зависимости от типа вредоносного програмного обеспечения, существует несколько сценариев, которые мошенники используют для атаки на пользователя. В конечном итоге все они приводят к тому, что вредоносные программы пытаются создавать и выполнять мошеннические действия от Вашего имени.

Какие меры предпринять?

- Храните свой ПИН-код и сгенерированный системой код в секрете. Никогда не раскрывайте эти секретные коды тем, кто их запрашивает, например: по телефону, по email, через SMS, WhatsApp или лично. Сотрудники ИНГ никогда не станут спрашивать у Вас эти коды.
- Никогда не генерируйте промежуточный защитный код, если вас об этом просит кто-то другой.
- Всегда проверяйт детали платежа, который подписываете, например номер счета получателя и сумму.
- Всегда нажимайте кнопку «Выход из системы» когда завершаете сеанс работы с Банк-Клиентом. Блокируйте компьютер когда оставляете его без присмотра во время активного сеанса

Правильное управление денежными средствами через Банк-Клиент

Определенное поведение пользователей Банк-Клиента может посодействовать мошенникам:

- Недостаточное внимание к контролю совместного подписания платежа: Совместное подписание является средством выявления и предотвращения мошенничества. Сотрудник, который подписывает платеж второй подписью, повторно проверяет реквизиты, которые заведены в систему другим сотрудником, тем самым у него больше возможности выявить мошенничество с этим платежом. Никогда не оставляйте обе подписи в руках одного и того же сотрудника и всегда проверяйте, что Вы подписываете. Всегда проверяйте, чтобы первый и второй подписант использовали разные ПК при подписании платежа, так как это увеличит шансы обнаружения мошеннических платежей, созданных вредоносными программами.
- Общий доступ: Не используйте устройства с общей авторизацией. Это повысит безопасность компании, так как сотрудник сможет действовать только в рамках своих полномочий.

Мошенничество с помощью приемов социальной инженерии, что это?

С помощью социальной инженерией можно так манипулировать человеком, что он раскрывает конфиденциальную или секретную информацию. Мошенник притворяется руководителем высшего звена или помощником руководителя с целью манипулирования сотрудниками для обработки ими платежа или для разглашения конфиденциальной информации.

Что происходит?

1. Мошенники связываются с Вашей компанией по электронной почте или по телефону, представляясь аудиторами, дипломированными бухгалтерами или даже государственными служащими, проводящими расследование. В процессе общения они собирают информацию о внутренних правилах отправки платежей компании, а также о сотрудниках, которые вовлечены в этот процесс. Кроме того, информация в социальных сетях (LinkedIn, Facebook, VK, ...) может помочь мошенникам выявлять сотрудников, вовлеченных в процессы формирования и отправки платежей, или отслеживать отпуска таких сотрудников с намерением выдать себя за них.
2. Мошенники связываются с сотрудниками компании, которые уполномочены подписывать платежи на крупные суммы, выдают себя за руководителей высшего звена и срочно, с максимальной секретностью, просят отправить платеж на крупную сумму (например, ссылаясь на решение о поглощении конкурента или т. п.).
3. Мошенники также могут представиться внешним консультантом, назвавшись, для правдоподобности, известным именем. Затем «консультант» связывается с сотрудником, уполномоченным проводить платежи, чтобы подтвердить сделку, говоря о ее секретности и срочности оплаты. Если сотрудник колеблется, мошенники будут использовать уловки, такие как увольнение руководителей компании, лесть или даже угрозы.

Какие меры предпринять?

- Относитесь всегда с осторожностью когда вас просят срочно и секретно провести платеж.
- В случае отклонения от стандартного запроса всегда звоните человеку, который отправил первоначальный запрос, по известному, предварительно проверенному номеру.
- Разделите обязанности подписывать платежи на нескольких сотрудников. Также всегда соблюдайте свои внутренние процедуры подписи платежей, не подписывайте платеж на доверии.
- Не разрешайте сотрудникам передавать персональные ключи доступа друг другу (сертификаты, ПИНы).
- Попросите сотрудников ограничить себя в публикации в социальных сетях деталей своей работы.

Разновидность такого мошенничества

Мошенники такого типа выдают себя за адвокатов, нотариусов, полицейских, службу поддержки и т. д.

Мошенничество с выставлением счетов, что это?

Мошенничество со счетами многообразно. Во всех случаях мошенники намериваются изменить реквизиты Вашего контрагента на свои, чтобы в результате получить оплату вместо него.

Что происходит?

1. Злоумышленники перехватывают выставленный счет в промежутке между его отправкой и получением. Для этого они взламывают электронную почту Вашего поставщика, регистрируя похожий на нее домен (мошеннический метод известен под названием domain typo squatting), и выдают себя за него.
2. Мошенники меняют реквизиты на свои. Поддельный счет перенаправляется жертве.
3. Жертва оплачивает счет по поддельным банковским реквизитам. Весьма вероятно, что последующие счета будут оплачены также на реквизиты мошенника, пока реальный поставщик не поймет, что его счета не оплачивают, и напрямую не свяжется с покупателем.

Какие меры предпринять?

- Проверка реквизитов счета: ожидали ли вы выставление счета? Не изменились ли данные поставщика в сравнении с предыдущими платежами?
- Любые изменения данных поставщика (адрес, номер телефона, адрес электронной почты, номер расчетного счета и т. д.) должны быть перепроверены с помощью звонка на подтвержденный номер (а не на тот номер, который указан в новом счете).

Варианты такого мошенничества

Например, компания-покупатель получает электронное письмо от поставщика, в котором говорится, что банковские реквизиты поставщика изменены. Сообщение будет выглядить вполне правдоподобным, потому что реквизиты будут пропечатаны на фирменном бланке. В подобных случаях все счета, ожидающие оплату этому поставщику, а также последующие счета будут оплачены по новым реквизитам.

Каким бы ни был сценарий, цель преступников состоит в подмене контактов и банковских реквизитов поставщика (номер телефона, банковские реквизиты, адрес электронной почты) для кражи денег.

Ограничение ответственности

Данная памятка предоставляется вам исключительно в информационных целях, чтобы Вы имели представление о наиболее распространенных случаях мошенничества и могли ознакомиться с предлагаемым руководством по защите своих интересов. Эта информация не гарантирует, что Ваша компания, действующая на основе этих рекомендаций, будет защищена от любого вида мошенничества, упомянутого в настоящей памятке. Никакие права не могут быть получены в связи с использованием мер предосторожности, которые Вы предпринимаете, выполняя рекомендации, указанные в настоящей памятке. ИНГ не принимает никаких обязательств и не несет ответственность в связи с использованием данной памятки и/или действиями, которые Вы предпринимаете в связи с использованием рекомендаций, указанных в настоящей памятке.