

Что делать в случае мошенничества?



Если вы подозреваете, что происходит мошенничество, незамедлительно сообщите об этом вашему клиентскому менеджеру или по телефону клиентской службы: т.: +7 495 937 7903 (пн-пт: с 9:00 до 17:30)

Или воспользуйтесь ящиком:

e: anti-fraudRU@ing.ru.

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.

Для оперативной блокировки доступа к Системе «ИНГ Бизнес» необходимо уведомить Банк по телефону «Поддержки клиентов» и/или направить уведомление по системе «ИНГ Бизнес».

Что делать в случае сомнений?

Лучше перестраховаться, чем потом пожалеть: о любом подозрительном платеже, нестандартном/неузнаваемом интерфейсе страниц сайта Банка/ интернет-банкинга, сомнительной коммуникации и т.п. следует уведомить ИНГ.

Что если ИНГ обнаружит подозрительную активность?

Если ИНГ заметит подозрительную активность, например, сомнительные (неудачные) попытки входа в систему интернет-банкинга или нетипичные платежи, представитель банка свяжется с вами для дополнительного подтверждения операций. Если у вас появятся сомнения относительно личности звонящего, перезвоните в Банк клиентскому менеджеру, используя контакты, представленные на официальном сайте Банка.



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 счетов.

Наша роль

В случае подтверждения факта совершившегося мошенничества мы будем помогать вам общаться с банком-получателем и предпринимать все возможные действия для приостановки зачисления денежных средств и их возврата. После получения сообщения банк-получатель будет проводить расследование и решит, какие действия могут быть предприняты с платежом в соответствии с применимым законодательством.

Мы, со своей стороны, также проводим все необходимые мероприятия по противодействию мошенничеству и стараемся обеспечить, чтобы никакие подозрительные операции не были проведены без вашего добровольного согласия и подтверждения.

Как использовать эту памятку?

Распространите ее в своей компании, чтобы повысить осведомленность 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!

Защитите себя от мошенничества

Узнайте о наиболее частых случаях мошенничества 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.



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?

- 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 интернет-банк.
- Поддельная контекстная реклама в поисковых системах: когда вы вводите в поисковую систему запрос, например, "ИНГ Банк", в качестве первого результата может появиться контекстная реклама, ведущая на поддельную страницу ИНГ. Такие поддельные страницы практически неотличимы от настоящих, а их адрес может отличаться всего на один символ.
- Перейдя по этой ссылке вы попадаете на мошеннический сайт, где вас могут попросить ваши персональные данные/ логин и пароль для входа в интернет-банк, 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 интернет-банк 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.

Какие меры предпринять?

Всегда проверяйте, ведут ли результаты поиска и рекламные объявления на безопасный и надежный сайт ИНГ.

- Убедитесь, что вы перешли на правильную страницу входа в систему интернет-банкинга: business.ing.ru/ru/html/login.html

- Кроме URL, проверьте также наличие замка в адресной строке вашего браузера. Это означает, что соединение безопасно, и вы можете проверить, что сертификат был выдан ING Groep N.V.

- 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 проверяйте детали платежа, который подписываете, например, номер счета получателя и сумму.

- Всегда нажимайте кнопку «Выход из системы», когда завершаете сеанс работы с интернет-банком.

Правильное управление денежными средствами через интернет-банк Определенное поведение пользователей интернет-банка может поспособствовать 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 возможностей 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

В зависимости от типа вредоносного программного 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.



Мошенничество с помощью приемов социальной инженерии, что это?

Социальная инженерия позволяет мошеннику получить конфиденциальную информацию или подтолкнуть жертву к каким-либо действиям путем различных манипуляций. Например, мошенник притворяется руководителем высшего звена или помощником руководителя с целью получения конфиденциальной информации или даже принуждения к совершению финансовых транзакций

Что происходит?

1. Мошенники связываются с вашей компанией по электронной почте или по телефону, представляясь аудиторами 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 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.
- Обеспечьте разделение обязанностей по формированию платежей между несколькими сотрудниками. Также всегда соблюдайте свои внутренние процедуры подписи платежей, избегайте платежей на основании устных договоренностей.
- Не разрешайте сотрудникам передавать персональные ключи доступа друг другу (сертификаты, ПИНЫ).
- Попросите сотрудников ограничить публикацию в социальных сетях деталей своей работы.

Разновидность такого мошенничества

Мошенники такого типа выдают себя за нотариусов, полицейских, сотрудников ФССП, прокуратуры, служб поддержки и безопасности банков и т. д.

Мошенничество с выставлением счетов, что это?

Мошенничество со счетами многообразно. Во всех случаях мошенники намериваются изменить подлинные 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, 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

- Не оплачивайте счета, содержащие реквизиты, отличные от согласованных в договоре с контрагентом, предварительно не подтвердив их.
- Любое изменение реквизитов телефона, контактов и поставщика (номера банковских реквизитов, электронного адреса и т.д.) должно сопровождаться звонком по номеру, указанному в полученном счете или сообщении

Варианты такого мошенничества

Например, компания-покупатель получает электронное письмо от поставщика, в котором говорится, что банковские реквизиты поставщика изменены. Сообщение будет выглядеть вполне правдоподобным. В подобных случаях все счета, ожидающие оплату этому поставщику, а также последующие счета могут оказаться 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) и получения оплаты за него.

Ограничение ответственности

Настоящий буклет является документом справочного характера и не составляет какого-либо обязательства, обещания или совета с нашей стороны.

Настоящий буклет является кратким обзором определенных вопросов, и не должен рассматриваться в качестве консультации. ИНГ БАНК (ЕВРАЗИЯ) АО (далее – ИНГ Банк) настоятельно рекомендует привлечь для соответствующих консультаций независимых профессиональных консультантов (юридических, консультантов по безопасности и т.п.).

ИНГ Банк не ручается за полноту и достоверность изложенных в настоящем буклете сведений. Настоящий буклет не является заверением относительно каких-либо обстоятельств. Любая информация, содержащаяся в настоящем буклете, должна использоваться исключительно в справочных целях и рассматриваться как предположение, без ручательства за достижение конкретного результата.

ИНГ Банк не принимает на себя никакой ответственности за убытки, связанные с использованием содержащихся в настоящем буклете сведений.

ИНГ Банк сохраняет все интеллектуальные права относительно информации, содержащейся в настоящем буклете.