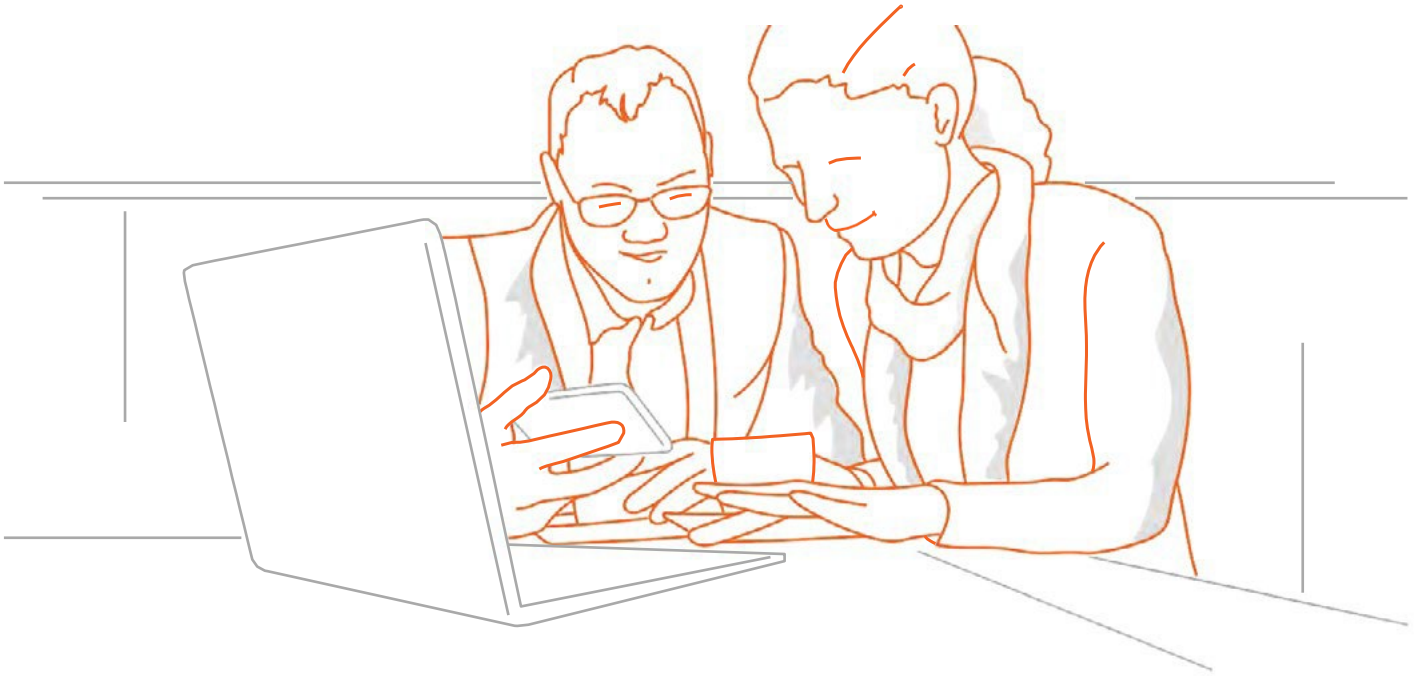
Что делать в случае мошенничества?



Если вы подозреваете, что происходит мошенничество, незамедлительно сообщите об этом вашему клиентскому менеджеру. 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.

Что делать в случае сомнений?

Лучше перестраховаться, чем потом пожалеть: о любом подозрительном платеже, нестандартном/неузнаваемом интерфейсе интернет-банкинга, сомнительном сообщении 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 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 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 подтверждения факта мошенничества мы будем помогать вам общаться с банком-получателем и предпринимать все возможные действия для приостановки зачисления денежных средств или 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 дополнительные проверки, чтобы выявлять подозрительную активность.

Как использовать эту памятку?

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. 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 интернет-банк.
2. Поддельная контекстная реклама в поисковых системах: когда вы вводите в поисковую систему запрос, например, "login InsideBusiness", в качестве первого результата может появиться контекстная реклама, ведущая на поддельную страницу ИНГ или InsideBusiness. Такие поддельные страницы практически неотличимы от настоящих, а их адрес может отличаться всего на один символ.
3. Перейдя по этой ссылке, вы вводите свой логин и пароль, для входа в интернет-банк, тем самым раскрывая их мошеннику для отправки платежа от вашего имени с вашего счета.

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 проверяйте все детали платежа, номер счета получателя и сумму;
- всегда нажимайте кнопку «Выход из системы», когда завершаете сеанс работы с интернет-банком;
- по возможности избегайте использования общедоступных Wi-Fi сетей при совершении операций в системе интернет-банка.

Варианты такого мошенничества

1. 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.
2. 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 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 — это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и является очень эффективным.

С помощью социальной инженерии можно так манипулировать человеком, что он раскрывает конфиденциальную и секретную информацию.

Социальная инженерия как наука динамично развивается, позволяя регулировать человеческое поведение и осуществлять контроль, но гораздо дольше она существует как методология атак. Профессионалы в этой области успешно обманывали людей на протяжении нескольких десятилетий, и всегда ставка делалась на человеческий фактор: любопытство, лень, страх. Чтобы не попасться в ловушку мошенников, нужно уметь распознавать основные приемы хакеров и понимать, что сведения, которые появляются в открытом доступе, могут быть использованы против тех, кто ими поделился.

Что происходит?

Мошенник притворяется сотрудником банка, социальных служб, сотрудником ритейловой компании и т. д. Мошенник связывается с вами при помощи электронной почты, сервисов мгновенных сообщений или SMS, посылая так называемое «фишинговое» сообщение, в котором напрямую просит вас предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносного ПО при нажатии ссылки и т. д.), благодаря чему получает желаемое часто при полном неведении с вашей стороны.

Какие меры предпринять?

- будьте осторожны при работе с вложениями из незнакомых источников;
- никогда не генерируйте промежуточный защитный код, если вас об этом просит кто-то другой;
- научитесь говорить: «Нет!». Вежливое отклонение запроса о получении доступа к вашей личной конфиденциальной информации поможет избежать многих проблем;
- будьте осторожны и предусмотрительны при общении в социальных сетях.

Разновидность такого мошенничества

Социальная инженерия в социальных сетях

С повышением роли социальных сетей в жизни людей в них успешно применяются методы социальной инженерии. На личных страничках люди добровольно сообщают факты о себе и своих близких, охотно вступают в контакт даже с посторонними людьми, не предполагая, что возможно ваш собеседник представляется не тем, кем является на самом деле и информация, которую вы добровольно о себе сообщаете, будет использована вам во вред. Также мошенникам легко создать поддельную страницу любой влиятельной организации или известной фирмы и расставлять там свои «капканы». В открытом доступе все на виду, но ничего нельзя проверить. В социальных сетях работают приемы социальной инженерии, основанные на любопытстве (желание зайти на интересную страницу, попытаться узнать больше о другом пользователе) и страхе (мошенники представляются сотрудниками правоохранительных органов и требуют доступ к аккаунту или просто предлагают установить антивирус). Атака социальной инженерии успешна, если мошенник действует смело и дерзко.