**КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ**

**ОСТОРОЖНО! МОШЕННИКИ!**

**По статистике каждый десятый телефонный звонок в России делается злоумышленниками. И многие из таких бесед по телефону заканчиваются для потенциальных жертв потерей денег. На первом месте лидируют звонки от имени сотрудников банков.**

**Прервите разговор и позвоните в свой банк**!

Перезвонить не на номер, с которого вам позвонили, а на номер банка. Вы попадете к официальному представителю и будете решать вопрос именно с ним, а не с человеком, который позвонил якобы от «банка».

**ЭТО МОШЕННИКИ! НЕ ВСТУПАЙТЕ В ДИАЛОГ!**

Вам на сотовый телефон поступает звонок от имени сотрудника банка, который сообщает, что в настоящее время по вашей банковской карте проходят подозрительные операции. Для того, чтобы их предотвратить необходимо назвать номер банковской карты и код, который придет в смс-сообщении.

Мошенники звонят или отправляют смс-сообщения часто с номеров, идентичных официальным банковским, благодаря подмене номеров.

**«Банки никогда не позвонят с вопросами о том, проводит ли клиент такую операцию. Банки сначала блокируют, а потом выясняют с клиентом, что происходит.**

**Помните!** Реальный сотрудник банка никогда не спросит вас о количестве карт и остатках, не попросит назвать пароли и коды из СМС, а также CVС-код (код безопасности) для проведения верификации. Сотрудник банка никогда не будет убеждать вас перевести деньги на некий резервный счет и не станет переключать вас на робота или коллегу, чтобы вы продиктовали пароли якобы в защищенном режиме или совершили операции «под контролем». Сотрудники службы безопасности банка могут позвонить вам, но также никогда не будут запрашивать какие-либо данные карт, их владельцев, CVС-коды.

Как противостоять мошенникам? Верный способ всего один — вообще не разговаривать с ними и тем более не выполнять никаких инструкций. Кто бы ни звонил и что бы ни говорил. Просто положите трубку и сразу же сами позвоните в свой банк по официальному номеру — он есть на оборотной стороне вашей банковской карточки. Сообщите оператору о подозрительном звонке. Банк проверит, все ли в порядке с вашей картой. Это не займет много времени и позволит вам сохранить ваши деньги.

**Правила безопасности**

**Как понять, что вам позвонил не настоящий сотрудник банка, а мошенник?**

1. Если по телефону вас просят сообщить реквизиты банковской карты или совершить какие-то операции с ней или счетом (через банкомат или мобильное приложение), вам позвонил мошенник, а не сотрудник банка. Настоящие сотрудники банка никогда не попросят об этом.  
     
   2. Если под каким-то предлогом вас просят назвать код из СМС-сообщения, вы столкнулись с мошенничеством. Банки никогда не спрашивают у клиентов коды и всегда в сообщениях пишут о том, что передавать их никому нельзя.  
     
   3. Если под предлогом защиты личного кабинета на сайте банка вас просят перейти по ссылке и авторизоваться. Скорее всего, вы попадете на сайт-клон. Визуально он может быть один в один похож на настоящий сайт банка. Введя данные, вы просто «сдадите» их мошенникам.  
     
   4. Если вас пугают сообщениями о том, что кто-то оформил на вас кредит, и предлагают выполнить ряд действий, которые якобы аннулируют этот кредит или позволят не платить проценты по нему.

**Если раньше мошенники были нацелены на банковские карты, то сейчас — на депозитные счета. Злоумышленники понимают — там денег гораздо больше.**

— **Депозитные счета — это сбережения**. Сценарий такой: звонок якобы из банка, клиенту сообщают, что поступило заявление о закрытии его депозитного счета. Человек поясняет, что такого заявления не подавал. Ему говорят, что сейчас все деньги с его депозита будут куда-то направлены в связи с его закрытием и предлагают перевести на «безопасный счет». И человек все свои деньги переводит на счет мошеннику.

Сценариев обмана очень много — мошенники весьма изобретательны. Но все схемы, как видно из примеров, объединяет одно: злоумышленники пытаются усыпить бдительность жертвы, оперируя личными данными человека, и используют психологическое давление. Они сообщают человеку об угрозе, которая нависла над его деньгами, заставляют запаниковать. Затем начинают давить, торопить, пугать: «счет идет на секунды…», «если вы не назовете код из СМС, мы не сможем спасти ваши деньги…» — подобные фразы не дают жертве возможности опомниться и подумать.

**Сегодня мошенники вовсю пользуются площадками, где торгуют персональными данными владельцев банковских карт. Так что под угрозой находится каждый потребитель финансовых услуг.**

**На втором месте по частоте использования — обман через покупки в интернете.** Главным образом на сайте объявлений, вроде Авито и «Юлы», и в социальных сетях. Контакта с жертвой у мошенника как такового нет, все происходит через переписку.

— Мошенник покупает за деньги виртуальный номер, на который регистрирует мессенджер, и переписывается с покупателем. У него даже симки нет на руках. Потерпевшему кидают ссылку — якобы для проведения безопасной сделки. Переходя по ссылке, которая сгенерирована мошенниками, граждане думают, что, введя данные своей карты, получат деньги, а на самом деле они списываются у них.

В арсенале мошенников — множество проверенных временем схем обмана, но есть и новые. К примеру, стала популярной тема инвестиций, и преступники тут же воспользовались интересом граждан в своих целях.

— Граждане начинают инвестировать сбережения в те или иные организации, в интернете есть масса предложений по этой тематике. Люди не разбираются и попадают в сети мошенников, которые выдают себя за инвесторов и обещают хорошую прибыль.

**Потерять деньги легко, а вот вернуть почти невозможно!**

— Возврат возможен в крайне редких случаях. Поскольку зачастую граждане сами предоставляют персональные данные своих банковских карт и сами производят переводы.

**Еще одна проблема: когда жертва сама делает перевод мошеннику, банк не может сразу заморозить операцию.**

— Клиенту после такого перевода нужно сразу обратиться в отделение банка или позвонить по горячей линии, сказать свои данные, чтобы операцию попытались заблокировать. Тут же попытаться заблокировать свое мобильное приложение или банковские карты, чтобы деньги до конца не списались. В банке нужно запросить выписку по счетам, это будет доказательством ого, что деньги ушли на другой счет. С этим документом можно будет обратиться в органы внутренних дел.

**Основная проблема в таких ситуациях — большая скорость операций.**

— Как только деньги уходят на получателя, через очень короткое время их уже там нет. Вопрос в том, чтобы остановить их на первом получателе. Но ни один банк не может бесконечно отслеживать всю цепочку переводов злоумышленников, особенно если это межбанковские платежи. Сейчас все операции могут занимать доли секунды, что сильно осложняет ситуацию.

Необходимо помнить, что все одноразовые пароли из СМС предназначены только для расходных операций и отправляются только для клиента. Назвать код из СМС вас попросят только мошенники. Если вы все-таки разгласили данные карты, пароли или выполнили инструкции мошенников, нужно немедленно обратиться в банк. Там сделают все возможное, чтобы предотвратить дальнейшие списания средств со счета и дадут рекомендации, что делать дальше.

Если с вашей банковской карты списали деньги, и **вы к этому не причастны**, как можно скорее позвоните в банк (номер есть на обороте карты), сообщите о мошеннической операции и заблокируйте карту. Обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме. Обратитесь в правоохранительные органы с заявлением о хищении. Получив ваше заявление, банк проведет служебное расследование и решит вопрос о возмещении ущерба. Если вы соблюдали меры безопасности и обратились в банк не позже, чем через сутки после списания денег, то можете рассчитывать на возмещение. Однако если вы сами сообщили злоумышленникам ПИН-код или код из СМС, необходимый для подтверждения платежей и переводов, к сожалению, вернуть деньги не удастся.

За получением подробной консультации и правовой помощи  потребители

могут обращаться:

— в Общественную приемную Управления Роспотребнадзора по Новгородской

области по телефонам 971-106;

— в Центр по информированию и консультированию потребителей  ФБУЗ «ЦГи Э

в Новгородской области» по телефону 77-20-38, 73-06-77;

Е-mail: [zpp.center@yandex.ru](mailto:zpp.center@yandex.ru); ВК: vk.com|zppnovgorod

— на «горячую линию» Единого консультационного центра Роспотребнадзора,

который функционирует в круглосуточном режиме, телефон 8 800 555 49 43

(звонок бесплатный).