**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**

**(БАНК РОССИИ)**

**Отделение по Пермскому краю Уральского главного управления**

614990, г. Пермь, ул. Ленина, 19

[www.cbr.ru](http://www.cbr.ru)

**ПРЕСС-РЕЛИЗ**

**Банк России обращает внимание: в Пермском крае, как и по всей России, участились случаи телефонного мошенничества**

***Мошенники научились подделывать номера горячих линий кредитных организаций и все чаще маскируют свой номер под официальные номера банков. Звонят с номера банка и просят предоставить конфиденциальные данные. Что делать? Разбираемся, как не попасться на уловки мошенников.***

Для начала проверьте, точно ли это сотрудник банка. Спросите его ФИО, название подразделения и скажите, что перезвоните позже. Обязательно прервите звонок и положите трубку. Даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Перезвоните по официальному номеру горячей линии банка (который есть на сайте или на обратной стороне банковской карты) и попросите соединить с тем сотрудником, который вам звонил. Наберите номер банка вручную.

Точно так же следует поступить, если вы получили СМС-сообщение, письмо на электронную почту или любое другое уведомление от имени банка.

***Алексей Моночков, управляющий Отделением Пермь Уральского ГУ Банка России.***

*- К сожалению, выявляется все больше случаев телефонного мошенничества со звонками якобы из коммерческих банков, все больше людей теряют свои деньги. Мошенники используют специальное программное обеспечение и цифровую телефонию которое помогает скрыть настоящий номер звонящего, при этом на телефоне человека отражается официальный номер банка. Обычно преступник обращается к собеседнику по имени и отчеству, может назвать фамилию и даже номер и срок действия карты. Эти сведения мошенники, как правило, получают заранее из открытых источников, например из социальных сетей, и с помощью* [*фишинга*](https://fincult.info/articles/moshennichestvo-bankovskimi-kartami/moshennichestvo-s-bankovskimi-kartami-online/)*.*

*Даже если информация звучит очень правдоподобно, лучше перестраховаться и позвонить в банк самому, чтобы общаться точно с его сотрудником, а не с преступником.*

Чаще всего мошенники звонят поздно вечером, ночью или ранним утром в выходные дни, когда человек спит и не может быстро сориентироваться. Преступник представляется сотрудником банка и сообщает о подозрительной операции, которая требует немедленных действий со стороны клиента. Мошенники хорошо знакомы с психологией: говорят быстро и уверенно, используют профессиональные термины, нередко фоном включают звуки, имитирующие работу оживленного колл-центра. Все это помогает им втереться в доверие к клиенту банка и сделать так, что он потеряет бдительность.

При этом они требуют немедленного ответа, торопят и запугивают клиента, давят на его эмоции и уверяют, что случится что-то непоправимое. Эти действия являются явным признаком мошенничества.

2

Например, мошенники говорят, что по карте проводится подозрительный платеж на крупную сумму и чтобы его остановить, нужно срочно сообщить данные карты, ПИН-код или одноразовый пароль из СМС-сообщения. Если человек колеблется или отказывается их назвать, ему угрожают, что деньги с его карты прямо сейчас уйдут к мошенникам.

Если преступникам удается узнать нужную им информацию, они получают доступ к счету и снимают с него все деньги.

**Как защитить свои деньги от мошенников?**

Если клиент сам сообщит преступникам секретную информацию, которую нельзя разглашать, вернуть деньги через банк не получится. Поэтому стоит придерживаться основных правил безопасности, чтобы не поддаться на уловки мошенников и не потерять деньги:

* Всегда набирайте только официальный номер банка. Он указан на обратной стороне карты и на официальном сайте банка.
* Не перезванивайте и не отправляйте СМС на незнакомые номера, не спешите переходить по ссылкам из сообщений «от банка». В любой непонятной ситуации звоните в банк по официальному номеру и уточняйте информацию у оператора.
* Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную.
* Не стоит паниковать и спешить. По действующему законодательству, если банк выявит подозрительную транзакцию, он сразу приостановит ее на срок до двух суток. Дополнительного согласия клиента на блокировку не требуется.
* Сразу после блокировки банк должен сообщить клиенту о случившемся. Это может быть звонок, СМС-сообщение, push-уведомление в мобильном приложении банка. В случае если банковская система защиты приняла операцию клиента за сомнительную по ошибке, то нужно подтвердить, что клиент действительно ее проводит. При этом операторы не просят называть кодовых слов и кодов из СМС.
* Это решение необходимо принять в течение 48 часов – этого времени достаточно, чтобы хорошо все обдумать и без спешки самостоятельно позвонить в банк. Если же вы ничего не сделаете, то через двое суток банк автоматически снимет блокировку и операция пройдет.
* Ни под каким предлогом никому не сообщайте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.

Пресс-служба Отделения Пермь Уральского ГУ Банка России

*19 июня 2019 года Пресс-служба*

*(342) 218-72-30*

*57media@cbr.ru*

[*http://www.cbr.ru/tubr/ural-o/news/*](http://www.cbr.ru/tubr/ural-o/news/)

*новости регионов Урала на сайте Банка России*