Пять шагов

Если всё же вы попались на удочку мошенников и сами перевели им деньги или увидели, что с вашей карты происходят сомнительные операции, не поддавайтесь панике и сделайте пять важных в такой ситуации шагов, советуют эксперты.

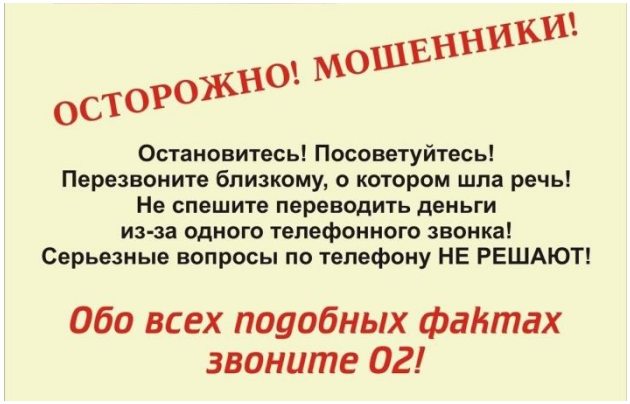
Шаг 1. Срочно заблокируйте карту через банковское приложение и смените пароль к нему. Это самый быстрый способ избежать дальнейших списаний средств. В противном случае мошенники могут вычистить ваш счёт.

Шаг 2. Как можно скорее обратитесь в службу поддержки банка. Во всех крупных банках поддержка работает 24 часа в сутки. Объясните детали произошедшего – это позволит службе безопасности отреагировать более оперативно, и шанс спасти ваши деньги значительно повысится.

Шаг 3. Обратитесь в полицию. Там нужно написать заявление о мошенничестве в отношении вас.

Шаг 4. Предупредите родственников и знакомых, что есть такой вид мошенничества. Это позволит уберечь их от возможных атак мошенников.

Шаг 5. Не принимайте звонки с неизвестных номеров хотя бы первое время после произошедшего. дело в том, что мошенники могут использовать подменные номера и каждый раз звонить с новой сим-карты. итак, будьте осторожны, сохраняйте спокойствие и бережно относитесь к своим персональным данным.



с. Юсьва,
ул. Красноармейская, 21
тел. 2-71-88, 2-84-33
E-mail: bib- uswa@mail.ru
Сайт библиотеки: http://usvalib.ru/
Режим работы:
с 09.00 до 18.00 ч.
Суббота: с 10.00 до 16.00 ч.
Выходной день: воскресенье
Тираж: 10 экз.
Составитель: Казанцева Л.Н.,
заведующий информационно-
библиографическим сектором
Юсьвинской центральной библиотеки

Муниципальное бюджетное учреждение культуры «Юсьвинская централизованная библиотечная система»

МОШЕННИК НА ПРОВОДЕ

Как не попасться на уловки телефонных аферистов

с. Юсьва
2025

Количество случаев телефонного мошенничества растёт. Вообще, преступления в сфере IT составляют больше 30 % от их общего количества.

Они могут представляться сотрудниками банка, соцзащиты, полиции, а также адвокатами, бывшими начальниками, старыми знакомыми и другими людьми, используя специальные программы для подмены голоса. Главное, понять механику их действий, тогда можно определить попытку обмана в звонке незнакомого человека.

Представляться людьми из спецслужб – типичная тактика мошенников. С одной стороны, это заставляет нервничать даже законопослушных граждан. С другой – так аферисты спекулируют на доверии к органам охраны правопорядка.

ЭТОГО ДЕЛАТЬ НЕЛЬЗЯ

Семь «НЕ». Это то, чего категорически нельзя делать. И если при разговоре вас просят сделать что-то из перечисленного – сразу кладите трубку и блокируйте таких незнакомцев.

1. **Не называйте** никогда и никому в телефонном разговоре данные своей банковской карты или код, который выслан вам по СМС. Данные карты и код подтверждения – ваш секрет.

Если назовёте, то любой человек может совершить операцию по вашим реквизитам. Найти его и вернуть деньги будет сложно.

2. **Не устанавливайте** приложения на телефон, когда вас просит сделать это незнакомый собеседник.

Это приложение может быть небезопасным.

3. **Не переводите** средства на незнакомые счета ни под каким предлогом. Тем более ни в коем случае не снимайте деньги со своих счетов, если вас просят положить их на незнакомый счёт через банкомат.

Даже если это банкомат крупного известного банка, от мошенничества он не убережёт.

4. **Не верьте** на слово. Даже если с обратной стороны провода говорят, что дело срочное, всегда сначала перепроверяйте информацию самостоятельно.

Мошенники давно научились подделывать телефонные номера при звонках – если вы начнёте искать номер звонящего в интернете, часто действительно найдёте его на сайте организации, сотрудником которой представился мошенник. Однако, это всего лишь маскировка. Государственные организации почти никогда не звонят самостоятельно, а если у них будет для вас важная информация, скорее всего, вы получите письменное уведомление.

5. **Не сообщайте** персональную информацию. Данные паспорта, СНИЛС, ИНН и других важных документов нельзя разглашать незнакомцам.

Они могут быть использованы злоумышленниками, например, для оформления микрокредита.

6. **Не отвечайте** на вопросы, употребляя простые слова «да» и «нет».

Некоторые банки вводят голосовые подтверждения по телефону с их помощью для совершения крупных финансовых операций. Поэтому мошенники собирают образцы разных голосов для подделки ответов от лица жертвы.

7. **Не используйте** ваши легко узнаваемые личные данные – такие, как дата или год рождения, последние цифры номера телефона и так далее, - в паролях к личным кабинетам и банковским приложениям.

Найти такую информацию в социальных сетях очень легко, и мошенники хорошо освоили перебор наиболее часто используемых комбинаций. Поэтому получить доступ к личному кабинету, где паролем будут ваша дата или год рождения, для них в комбинации с фишингом не составит практически никакого труда.

И помните: **сотрудники банка или органов власти никогда не попросит о переводе средств. А если что-то понадобится правоохранительным органам, то они вызовут повесткой. Следственные действия в России по телефону не ведутся!**