

Порядок действий в случае поступления звонков телефонных мошенников

Мошенники постоянно придумывают различные поводы и способы отъема денег у населения, как работающего (личные сбережения), так и у безработных и пенсионеров, путем оформления кредитов.

Наиболее распространенными способами являются звонки под предлогом сбережения ваших средств от несанкционированного списания, завладения вашими персональными данными другими лицами и попытками оформить кредит на ваше имя. При этом, звонящие могут представиться вам как сотрудниками правоохранительных органов (МВД, прокуратура, ФСБ, следственный комитет), и для подтверждения данного факта и введения вас в заблуждение, они порекомендуют вам зайти на сайт той или иной силовой структуры, и проверить номер, с которого звонит мошенник, так как данный номер там будет указан. Это означает, что мошенники звонят с подложных номеров-двойников, чтобы вас запутать, так как сотрудники полиции никогда не будут по телефону просить оказать содействие сотрудникам банка, а также угрожать, что если не переведете деньги, то в отношении вас будет возбуждено уголовное дело.

Зачастую злоумышленникам известны ваши персональные данные, такие как ФИО, возможно, даже данные банковских карт.

Также, в настоящее время очень распространенным стал способ, когда звонящие сообщают вам о том, что ваш личный кабинет на портале Госуслуг взломан и ваши персональные данные похищены; а также, что к вашей карте пытаются привязать другой абонентский номер, и чтобы этого не допустить, необходимо выполнить определенные действия, которые вам скажут мошенники.

Во всех перечисленных случаях, самым действенным способ избежать утраты своих денежных средств - это прервать диалог с указанными лицами, положить трубку и самостоятельно связаться с банком, а лучше доехать или дойти до филиала и уточнить все моменты.

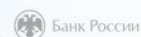
Также, распространены способы, когда обманывают посредством совершения покупок или продаж в соц. сетях (Авито, Юла), когда люди пытаются оформить доставку, не ознакомившись с правилами ее оформления (осуществляют предоплату напрямую, либо переходят по сомнительным ссылкам, в результате чего теряют свои деньги).

| | |
|--|--|
| Человек размещает в сети Интернет (Авито, Юла и прочие сайты) объявление о продаже чего-либо. Мошенники звонят по указанному номеру, представляются покупателями и просят сообщить данные карты для перечисления денег за покупку (либо перевести предоплату). | Никому не сообщайте номер карты или счета и тем более трехзначный код, расположенный на оборотной стороне карты, а также не передавайте SMS-код, который Вам приходит от номера телефона службы банка. |
| Вам звонят с незнакомого номера и тревожным голосом сообщают что ваши близкие попали в беду. А для того, чтобы решить проблему, нужна крупная сумма денег. | По такой схеме работают мошенники! Позвоните родственникам, чтобы проверить полученную информацию. |
| На Ваш телефон приходит анонимное сообщение от имени Вашего родственника, в котором просят пополнить баланс неизвестного номера. При этом, аноним просит не перезванивать и обещает связаться с Вами позже и все объяснить. | Ни в коем случае не выполняйте операций по переводу денежных средств! Сообщите о случившемся в полицию. |
| К Вам пришли работники социальных служб. | Прежде чем открывать входную дверь, позвоните в организацию, приславшую их. Мошенники занервничают, а настоящие работники отнесутся с пониманием. Никогда не отдавайте деньги, ценности и документы. |
| К Вам пришли лица, представившиеся медработниками либо сотрудниками Роспотребнадзора, ЖКХ (УК) и под предлогом проведения дезинфекции квартиры просят впустить в квартиру. | Позвоните в организацию, от которой пришли дезинфекторы по официальным номерам телефонов организации, размещенным на официальном сайте в сети Интернет и проверьте данную информацию. Сообщите о случившемся в полицию. |
| На сайте «Одноклассники», «ВКонтакте», «Инстаграмм», «Телеграмм» и др. Вам пришло сообщение от знакомого, с просьбой перевести определенную сумму денег. | Возможно, страница взломана мошенниками. Свяжитесь со знакомым по телефону и уточните, действительно ли ему нужна указанная сумма. |
| Брокерские сайты – звонят мошенники и предлагают открыть, а затем пополнить инвестиционный счет под высокие проценты | После звонка «брокера» нужно зайти на сайт брокера, изучать информацию в Центробанке. Лучше лично прийти в брокерскую фирму или банк. |
| Не доверяйте карты официантам или продавцам | Может быть предоставлен подложный QR-код или терминал мошенников |
| Мошенничество с автомобилями | Введение в заблуждение о техническом состоянии, взятие залога или предоплаты |

ОБЩИЕ ПРАВИЛА ЗАЩИТЫ ОТ КИБЕРМОШЕННИКОВ

1. Не сообщайте никому личную и финансовую информацию (данные карты).
2. Не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам.
3. Не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы.
4. Установите на все свои гаджеты антивирусные программы и регулярно обновляйте их.
5. Заведите отдельную банковскую карту для покупок в Интернете.
6. Самостоятельно звоните в свой банк по номеру телефона, указанному на оборотной стороне карты или на официальном сайте банка.
7. Установите двухфакторный способ аутентификации – например, логин и пароль + подтверждающий код из СМС.
8. Пользуйтесь только официальными сайтами финансовых организаций, в поисковых системах (Яндекс, Mail.ru) они помечены цветным кружком с галочкой.

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ



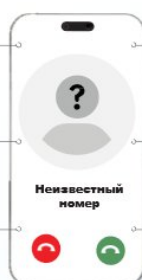
КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ



Не отвечайте на звонки
с неизвестных номеров

Прервите разговор,
если он касается
финансовых вопросов

Не торопитесь
принимать решение



Самостоятельно позвоните
близкому человеку / в банк /
в организацию

Проверьте информацию
в Интернете или обратитесь
за помощью к близким

Не перезванивайте
по неизвестным номерам



Возьмите паузу и спросите совета у родных и друзей!