ООО "Флекслайн-Н"
ИНН 5024055463 / КПП 502401001 / ОГРН 1025002876612
Юрид. и факт. адрес: 143401, Московская область,
г.Красногорск, ул.Международная, дом 2, помещение 1

Уважаемые абоненты!

В связи с участившимися случаями мошенничества и хищениями денежных средств с банковских счетов посредством использования средств телефонной связи, рекомендуем Вам быть внимательными!

Помните! Мошенники орудуют в следующих случаях:

Случай с родственником. Если Вам звонят и сообщают, что нужны деньги, чтобы спасти попавшего в беду родственника.

Медицина. Если Вам звонят и представляются сотрудниками медицинских учреждений, дистанционно ставят диагноз, при этом назначают курс лечения и предлагают приобрести лекарства.

Призы и компенсации. Если Вам звонят и сообщают, что вы выиграли приз или вам полагается компенсация, но для их получения необходимо перевести деньги на незнакомый вам счет.

Если Вам звонит незнакомец и просят конфиденциальные данные. Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка». Мошенник сообщает, что «банк производит выплаты», «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас **полные данные карты, CVV- или CVC-код, код из СМС, логины, пароли или просит установить программное обеспечение**. Это нужно якобы «для сохранности ваших денег».

Если Вам звонит робот — будто бы от банка. Он сообщает, что ваша карта «заблокирована в связи с подозрительной операцией», просит вас перезвонить для выяснения подробностей и диктует номер. По этому номеру отвечает мошенник под видом сотрудника службы безопасности — пугает вас потерей денег и настойчиво предлагает их «спасти», переведя на «безопасный счёт», либо старается выманить секретные данные (например, логин или код из СМС).

Если проводится опрос от Банка. Вы получаете письмо или СМС о том, что Банк проводит лотерею. Вам предлагают пройти опрос по ссылке, вы кликаете и попадаете на фишинговый сайт. Вы проходите «опрос» на сайте, и за это вам обещают крупную сумму вознаграждения, например, 150 тысяч рублей. Но для подтверждения карты и перечисления бонусов вас просят перечислить «закрепительный платеж» в размере 150 рублей. Вы отправляете деньги, а потом не можете связаться с мошенниками.

Если поступил звонок из прокуратуры. Мошенник звонит и сообщает, что некий сотрудник банка с доступом к вашему счёту находится под подозрением и в его отношении ведутся следственные действия. На следующий день мошенник звонит вам под видом «представителя прокуратуры». Он сообщает, что вам необходимо выполнить гражданский долг — помочь следствию, а также убеждает вас перевести свои деньги на «специальный счёт» для гарантии их сохранности.

Перевод по ошибке. Вы оставили своё имя и номер телефона на сайте бесплатных объявлений. Вскоре кто-то присылает вам с мобильного телефона СМС, подделанное под банковское сообщение об операции. Затем с другого номера приходит СМС с просьбой вернуть деньги.

Соблюдайте правила финансовой безопасности!

Как защитить себя

НЕ ОТВЕЧАЙТЕ И НЕ ПЕРЕЗВАНИВАЙТЕ ПО ПОДОЗРИТЕЛЬНЫМ НОМЕРАМ!!!

- Не совершайте никаких операций по инструкциям звонящего.
- Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), логины и пароли, коды из СМС, номер банковской карты, не попросит установить дополнительные программы.
- Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на доверенные номера и сообщите о случившемся.
- Запоминайте ваши пароли и нигде не записывайте их, время от времени меняйте пароль. Не используйте в качестве паролей номера телефонов, даты рождения, а также последовательность символов, расположенных подряд на клавиатуре.
- Внимательно читайте тексты СМС-сообщений с кодами подтверждений, проверяйте реквизиты операции.
- При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных сообщений от якобы «вашего банка (например, «Ваша карта заблокирована», «Заблокирована сумма оплаты», «Есть проблемы с проведением операции» и т.п.):

- ни в коем случае не перезванивайте на указанные в сообщениях номера,
- не сообщайте данные банковских карт: срок действия, контрольный код с обратной стороны карты, СМС-коды подтверждения, а также персональные сведения: серия и номер паспорта, адрес регистрации и пр.

В такой ситуации следует считать, что звонки или сообщения приходят от мошенников. Вам нужно прекратить контакт и самостоятельно обратиться в банк по доверенным телефонам.

- Не переходите по ссылкам на незнакомые ресурсы, не устанавливайте программы для удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin): мошенники могут заразить ваш компьютер или телефон вирусом, получить удалённый доступ к Вашим личным данным и финансам.

- Для использования веб-версии систем банков (Онлайн-банки) переходите на ресурс по ссылке, размещённой на официальном сайте вашего банка. При посещении сайта банка обращайте внимание на адресную строку https:// и наличие сертификата безопасности.
- При получении электронных писем от банка обращайте внимание на отправителя, наличие цифровой подписи.
- Используйте только официальные банковские приложения . Никогда не пользуйтесь другими неофициальными приложениями во избежание передачи личной информации мошенникам.
- Владельцам смартфонов настоятельно рекомендуем использовать антивирусное ПО, которое поможет уменьшить вероятность попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от банка СМС-сообщений, кражи персональных данных и авторизационных данных карты.

Если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обращайтесь в полицию!

Телефоны для связи: 02, 102 (с мобильного) или по единому номеру телефона спасения 112

Будьте бдительными! Не дайте себя обмануть!