Осторожно! Мошенничество по мобильному телефону!

- **Звонок от сотрудника «службы безопасности банка», «центра финансовой безопасности» и** т.п. **служб.** Поступает звонок об одобрении кредита, возврате страховки, о совершении подозрительного перевода. Просят назвать коды из (МС-сообщений непосредственно во время разговора либо переключают на голосового помощника, либо просят подойти к банкомату для совершения определенных действий.
- **Звонок от покупателя.** По размещенному объявлению о продаже поступает звонок от покупателя, который просит сообщить данные карты (логин/пароль, ПИН-коды, CVC2/CVV2 (последние 3 цифры на обратной стороне карты)) для перевода оплаты.
- **Просьба о помощи.** (МС-сообщение или пост в мессенджерах. Мошенники под видом близких родственников: «мамы», «друга», «сына» просят перевести определенную сумму на указанный номер.
- **Телефонный номер-грабитель.** Сообщение с незнакомого номера с просьбой перезвонить по любой причине - проблема со связью, смена тарифа, помощь другу и т.д. В случае обратного звонка с вашего счета спишется денежная сумма.
- **Ошибочный перевод средств.** Приходит (МС-сообщение о якобы поступивших средствах на счет. После этого поступает звонок или еще одно (МС-сообщение с просьбой вернуть деньги обратно, т.к. они отправлены по ошибке не на тот номер.
- **Требование выкупа.** Звонок с требованием выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

Правила безопасности

- **При звонке из «службы безопасности банка» или «центра финансовой безопасности» и т.п. служб ответьте, что перезвоните сами и положите трубку. Совершите звонок в банк по номеру телефона, указанному на обратной стороне банковской карты.**
- В случае каких-либо сомнений - не перезванивать по указанным номерам, не отправлять ответных (МС-сообщений, не переводить средства на незнакомые номера, никому не сообщать логин/пароль, ПИН-коды, CVC2/CVV2 (последние 3 цифры на обратной стороне карты), или другие коды, которые приходят,срокдействия карты.
- Важно помнить, что нельзя вводить свой номер телефона на незнакомых сайтах для регистрации или подтверждения какой-либо информации, а также устанавливать на телефоны приложения из неофициальных источников, не рекомендованных производителем мобильного телефона.
- Всегда связываться напрямую с близким или родственником, банком, оператором связи и т.д.
- Подключите сервис «Мобильный банк» или оповещение на адрес электронной почты для информирования о проводимых операциях.
- Будьте бдительными и помните о существовании мошеннических схем!

Осторожно! Мошенничество в сети Интернет!

- **«Друг» в социальных сетях** просит помощи или оплатить товар. Как правило, просят прислать номер вашей карты и код подтверждения операции.
- **Сайт-дублёр** - это сайт, который внешне повторяет настоящий сайт организации и имеет похожее написание имени сайта в адресной строке браузера.
- **Вредоносные программы** заражают смартфон или компьютер. При переводе денежных средств вирус показывает так называемые «веб-фейки» - окна браузера, визуально схожие с окнами авторизации банковских операций. При вводе в них данных банковских карт денежные средства отправляются злоумышленникам.
- **Электронные письма сомнительного характера.** Это могут быть письма с несуществующими вакансиями, просьбы отправить взнос за какие-либо дополнительные услуги, письма с назначением встречи в онлайн-календаре, письма-угрозы, в которых мошенники шантажируют, требуя перевести им денежные средства взамен конфиденциальной информации о вас.
- **Фишинг** - письма с предложением товаров, поддельные письма от представителей официальных организаций или банков. В сообщении просят предпринять незамедлительные действия, затрагивающие ваш аккаунт, например, подтвердить детали банковского счета, изменить пароль, получить приз. Может использоваться текущая ситуация (стихийные бедствия, финансовые проблемы, праздничные мероприятия), чтобы заставить перейти по ссылке или открыть вложение. Большинство фишинговых писем содержат ссылки на поддельные веб-сайты, с помощью которых похищаются конфиденциальные данные (логины, пароли, номера карт и т.д.), либо выполняется операция по перечислению денежных средств на счета злоумышленников.

Правила безопасного использования сети Интернет

- Быть бдительными и внимательными при получении сообщений или писем, в которых вас просят выполнить переводы средств или покупку чего-либо.
- Перепроверяйте любую полученную информацию.
- Не открывайте файлы-вложения от неизвестных отправителей.
- По возможности не сохраняйте в системе пароли и периодически меняйте их.
- Не переходите по гиперссылкам в письме.

При совершении операций через Интернет

- Не используйте ПИН-код при заказе товаров и услуг в Интернет, а также по телефону/факсу.
- Пользуйтесь Интернет-сайтами только известных и проверенных организаций торговли и услуг.
- Обязательно убедитесь в правильности адресов Интернет-сайтов, на которых собираетесь совершить покупки.
- По возможности совершайте покупки только со своего компьютера.
- Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление.

Осторожно! Мошенничество с банковскими картами!

- **«Ваша карта заблокирована!», «Совершен платеж».** Подобные (МС-сообщения приходят с неизвестных номеров. При звонке на указанный номер вас просят сообщить номер банковской карты, CVC2/CVV2 или ПИН-код.
- **Карта попала в чужие руки.** Любой продавец в магазине, кафе, на заправке может сфотографировать, переписать данные банковской карты или просто запомнить и передать мошенникам для изготовления дубликата карты.
- **Оплата дважды.** При расчете за покупку кассир сообщает об ошибке и просит повторно произвести оплату. Спустя какое-то время вы обнаруживаете, что деньги за покупку были списаны дважды.
- **Близнецы-«симки».** Этот способ используется, когда мошенники уже завладели данными карты и им необходимо при помощи кода из (МС-сообщения подтвердить транзакцию перевода денег на нужный счет. С помощью дубликата мошенники получают полный контроль над счетами, так как банковские карты, как правило, могутуправляться дистанционно с телефона.

Правила безопасного использования банковских карт

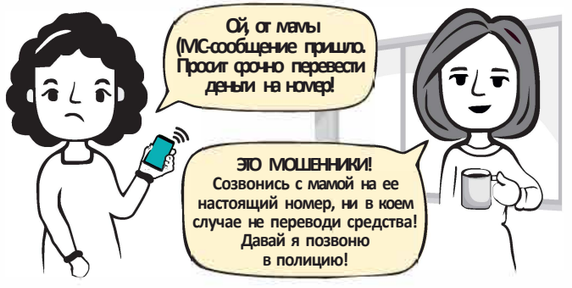
При оплате товаров и услуг

- Не выпускайте из поле зрения карту - все операции с картой должны проводиться на ваших глазах. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть.
- Кассир может потребовать предоставить паспорт, подписать чек или ввести ПИН-код. Перед тем как подписать чек, нужно в обязательном порядке проверить, чтобы сумма, снятая с карты, соответствовала сумме купленных товаров.
- Если при попытке оплаты банковской картой произошла «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.
- В случае любых сомнений безопасности использования карты лучше обратиться в банк с заявлением о ее перевыпуске.
- Установите индивидуальный расходный лимит по карте с бесконтактным платежом и ограничьте количество возможных транзакций.

При совершении операций в банкомате/инфокиоске

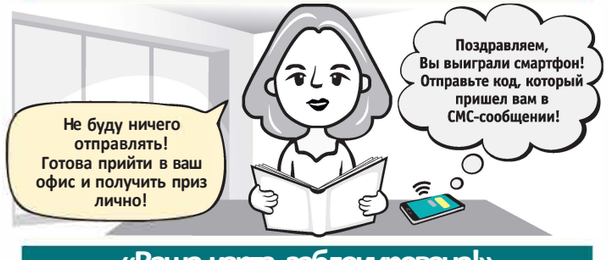
- Перед использованием устройства осмотрите его на наличие мошеннических устройств (накладок), расположенных в месте набора ПИН-кода и в месте, предназначенном для приема карт (прорезь). Если что-то покажется подозрительным, не используйте устройство. Сообщите о ваших подозрениях в службу поддержки банка, указав адрес расположения устройства, которое вызвало у вас подозрение.
- Набирайте ПИН-код так, чтобы стоящие рядом люди не могли его увидеть. Прикрывайте клавиатуру рукой.
- Запрещается ввод ПИН-кода в пропускные устройства для доступа в помещение, где расположен банкомат/инфокиоск.
- В случае захвата карты устройством необходимо заблокировать карту по телефону, указанному на сайте банка или через сервис «Интернет-Банк» или его мобильное приложение.
- В момент получения денег не отвлекайтесь на сторонние разговоры и звонки. Дождитесь выдачи денег, заберите и пересчитайте их.
- Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах/инфокиосках.

СМС-сообщения с просьбой о помощи



Телефонный номер-грабитель

Выигрыш в лотерее



«Ваша карта заблокирована!»