**Банковские карты и онлайн-платежи: базовые правила**

1. Никогда не сообщайте никому, даже сотрудникам банка, свои подтверждающие пароли из СМС, ПИН- и CVV-коды от банковских карт. Банк никогда не обращается с такими просьбами к своим клиентам. Не пишите ПИН-код на самой карте. Если все же хотите записать его на всякий случай, не храните эту запись в кошельке, а держите дома. Не стоит использовать в записке слова вроде «пин-код», пусть это будут просто четыре цифры, записанные в укромном месте.
2. Если вам позвонили (или написали) «из банка» и у вас возникли малейшие подозрения в том, что вам говорят, лучше ответить, что вам сейчас неудобно разговаривать, и перезвонить на горячую линию банка, а лучше наведаться в отделение.
3. Используйте только официальные банковские приложения из магазинов App Store, Google Play, Windows Store. Старайтесь не скачивать финансовые приложения, которые могут получить доступ к вашим данным (планировщики бюджета, приложения для онлайн-торговли и прочее) со сторонних ресурсов.
4. Используйте антивирус на телефоне и на компьютере и регулярно обновляйте его. Некоторые банковские приложения (например, «Сбербанк Онлайн» для Android) имеют встроенный бесплатный антивирус.
5. Не переходите по сомнительным ссылкам на незнакомые интернет-ресурсы: мошенники могут заразить ваш компьютер или телефон вирусом и украсть личные данные.
6. Переводите деньги только тем получателям, которые вам известны. Всегда проверяйте реквизиты операции в СМС от банка с подтверждающим паролем.
7. Подключите сервис СМС-информирования («мобильный банк»), чтобы всегда быть в курсе всех операций. Подключайте сервис только на свой номер телефона.
8. Если вы получили оповещение об операции, которую не совершали, позвоните в банк и заблокируйте карту. В случае потери карты также сразу ее заблокируйте. Номер контактного центра банка лучше сохранить в телефоне.
9. Если вы сменили номер мобильного телефона, не забудьте позвонить в банк и сообщить об этом, чтобы ваши данные не попали новому владельцу номера.
10. Для входа в зоны самообслуживания отделений банков не нужно вводить ПИН-код карты.
11. Информации, указанной на карте, достаточно, чтобы совершить с ее помощью покупку в интернете. Поэтому старайтесь не передавать свою карту в чужие руки и не выпускайте ее из виду при оплате покупок. В магазине самостоятельно вставляйте карту в терминал, в кафе позовите официанта с переносным ридером либо сами подойдите к кассе и расплатитесь.

**Безопасность при бесконтактных платежах**

Самая очевидная опасность при пользовании бесконтактной картой — ее потеря. Если она попадет в руки злоумышленника, тот сможет беспрепятственно совершать покупки до 1000 рублей, пока владелец ее не заблокирует (при покупках свыше этой суммы нужно обязательно вводить пин-код).

Несколько платежей подряд на мелкую сумму заставят сработать защитные системы банка, и тот может автоматически заморозить такие операции как подозрительные до подтверждения их легитимности.

Как правило, операция блокируется после трех совершенных подряд операций на сумму, не требующую пин-кода.

**Финансовое мошенничество в соцсетях**

**«Сотрудники банка», пишущие в личных сообщениях**

Стать жертвой кибермошенников можно не только в интернет-магазине или снимая деньги в банкомате. Мошенники могут использовать в своих целях и соцсети — например, представляться сотрудниками банка и предлагать поучаствовать в опросе банка за вознаграждение и призы, а после «опроса» попросить данные карты «для перевода денег», пароль от онлайн-банкинга или другие данные. Если бы эти люди были настоящими сотрудниками, у них и так были бы все необходимые реквизиты для перевода.

Банки никогда не запрашивают конфиденциальные данные в соцсетях. Максимум, что может запросить сотрудник банка, — только Ф.И.О., дату рождения или номер телефона, и то только в том случае, если клиент сам обратился с проблемой.

Если же кто-то от имени банка просит предоставить номер карты, скан паспорта или пароль от онлайн-банкинга — это мошенник.

Кроме того, банки никогда не предлагают призы или подарки в личных сообщениях. Когда вас зовут поучаствовать в играх с призами через личку, помните, что приз тут — ваши деньги и его хочет получить мошенник.

**«Легкий заработок» с тяжелыми последствиями**

Еще один вид мошенничества с картами через соцсети — дроперство. Мошенник публикует в соцсети объявление или пишет в личку, предлагая заработок за «залив» (или «обналичку»). Он просит номер карты, чтобы через нее перебросить деньги на другую или снять с нее поступившие средства в банкомате, и обещает за это заплатить.

Таким образом киберпреступники хотят найти дропера — того, кто даст свою карту для отмывания незаконных денег за небольшие комиссионные. Мошенник не хочет засвечиваться перед службой безопасности банка и полицией, поэтому ищет наивного человека, который хочет легко заработать и не думает о последствиях.

А последствия будут — банки следят за законностью денежных переводов и могут временно или навсегда отказать дроперу в обслуживании. Полиции тоже будет трудно объяснить, почему чьи-то «грязные» деньги прошли через вашу карту или карту вашего ребенка. А уголовную ответственность за соучастие в отмывании денег никто не отменял.

**«Помощь» в получении кредита**

Мошенник пишет в личку или публикует объявление, в котором обещает, что поможет получить кредит на льготных условиях — даже если вы в черном списке банков. Конечно, ни с каким кредитом он помогать не собирается. Ему нужны только персональные данные — скан паспорта, СНИЛС, ИНН и др.

Обладая такой информацией, можно, например, зарегистрировать на ваше имя электронный кошелек и вывести через него незаконно полученные деньги. А можно оформить кредитную карту в каком-нибудь нетребовательном банке, а потом вам придется доказывать, что вы тут ни при чем, либо расплачиваться по кредиту, который вы не брали.

Любые подозрительные или слишком заманчивые предложения в соцсетях нужно игнорировать. Еще лучше — пожаловаться на пользователя администрации социальной сети и отправить сообщение в официальную группу банка.

**Ложный друг**

Мошенники могут взломать страницу вашего знакомого или друга вашего ребенка в соцсети и вступить в переписку. Иногда они не сразу просят денег, а пытаются вовлечь в диалог.

«Друг» отвечает на сообщения коротко и неинформативно и довольно быстро просит о помощи (или просто взаймы), указывая реквизиты карты для перевода.

В таком случае лучше связаться с отправителем сообщения по другим каналам (смс, телефон, другие соцсети) и уточнить, действительно ли ему нужны деньги. Или задать в переписке вопрос, ответ на который может знать только друг, чтобы проверить, действительно ли это он.

**Внезапные выигрыши и интернет-лотереи**

Если вдруг вы оказались миллионным посетителем незнакомого сайта или получили письмо о выигрыше в лотерее, не спешите радоваться. Скорее всего это не что иное, как еще один из видов мошенничества с целью получить ваши персональные данные или деньги. Чтобы не стать его жертвой, соблюдайте простые правила.

1. Невозможно выиграть приз в лотерее, в которой вы не участвовали. Акции, в которых приз получает миллионный посетитель сайта, иногда действительно проводят крупные компании. Но информация о таком розыгрыше публикуется заранее и ее можно проверить по официальным источникам.
2. Любые просьбы «организаторов лотереи» об оплате налога или внесении иной суммы денег ДО получения приза — признак мошенничества. Все налоги и сборы выигравший платит сам ПОСЛЕ получения приза.
3. Тщательно проверьте всю информацию о розыгрыше в интернете: сведения о компании-организаторе, официальные правила розыгрыша, имена и телефоны отправителей сообщения. Иногда мошенники создают целые сайты с именами «победителей» — проверяйте адрес сайта и реквизиты компании-организатора.
4. Письма с ошибками или явно переведенные автоматическим переводчиком — еще один признак мошенничества. Проверьте e-mail, с которого пришло уведомление: организаторы лотерей не используют бесплатные почтовые сервисы, а пользуются доменом компании, которая проводит розыгрыш.

**Игры со встроенными покупками**

Многие бесплатные приложения предлагают совершать покупки в процессе игры, чтобы открыть новый уровень, увеличить скорость персонажа, получить редкие артефакты. К сожалению, детские игры — лидеры среди таких приложений.

Дети могут даже не подозревать, что игровая валюта — это реальные денежные средства, да и сами взрослые нередко забывают, что конвертируют виртуальные деньги в реальные.

Проблема в неконтролируемой трате средств: покупки во время игры кажутся особенно соблазнительными, а связь с реальными деньгами — неочевидной. Объясните ребенку, что на внутриигровые покупки тратятся реальные деньги и их сумма должна быть адекватной удовольствию от игры и возможностям семейного бюджета. Постарайтесь договориться, что если он захочет что-то купить во время игры, пусть сначала обратится к вам.

Лучшее средство защиты от чрезмерных игровых трат — по возможности не привязывать банковскую карту к устройству, на котором играете вы или ребенок. Если карта привязана, настройте функцию ограничения покупок. Инструкции для этого есть как для [телефонов на Android](https://support.google.com/googleplay/answer/1626831?hl=ru), так и для [устройств Apple](https://support.apple.com/ru-ru/HT204396).

**Платные подписки**

Платные (и условно бесплатные, затем переходящие в платные) подписки в приложениях на смартфонах тоже могут стать причиной незапланированных финансовых трат. Вовремя отключать или изменять платную подписку, если она вам больше не нужна, помогут опять же инструкции для [Android](https://support.google.com/googleplay/answer/7018481?co=GENIE.Platform%3DAndroid&hl=ru) и [Apple](https://support.apple.com/ru-ru/HT202039).

Не лишним будет также проверить статус подписок и платных услуг у мобильного оператора. Даже 100 рублей в месяц на ненужную услугу, о которой вы и не подозревали, за год превращаются в 1200 рублей, а в масштабах всей семьи это уже несколько тысяч.