ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

КАК ЗАЩИТИТЬ ДЕНЬГИ НА СВОЕЙ БАНКОВСКОЙ КАРТЕ

БС Банк

Телефонный звонок от сотрудника Центробанка

- *Мошенники представляются «сотрудниками» банка или Центробанка. Звонящий наверняка скажет, что на вас оформили кредит, — и даже может отправить в мессенджер документы с печатями, выписки из банка, судебные повестки. После он переведет звонок на «следователя», который занимается делом: тот подтвердит информацию и расскажет, что делать дальше. Для убедительности собеседник может отправить фотографии своего удостоверения.*

Ваши действия в данной ситуации

- *Не сообщать никаких данных, прерывать разговор. Помните, что Центробанк не работает с физическими лицами, а полиция никогда не отправляет фото документов в мессенджерах. После разговора с мошенниками лучше позвонить в свой банк, чтобы уточнить, все ли в порядке.*

БС Банк

Телефонный звонок от «старшего оперуполномоченного»

- *Ситуация: иногда мошенники могут представиться «старшим оперуполномоченным» или другим сотрудником МВД. Это пугает и дезориентирует. Собеседник скажет, что расследует дело об утечке персональных данных, в том числе ваших. Спросит, какими банками вы пользуетесь, какие операции проводили и на какие суммы. А в итоге попросит назвать данные карты, в том числе трехзначный код на обороте.*

Ваши действия в данной ситуации

- *Не сообщать никаких данных и положить трубку. Помните, что сотрудники МВД никогда не запрашивают номер карты, трехзначный код или код из СМС. Зато мошенникам эти данные откроют доступ к вашим деньгам.*

БС Банк

Мошенничество при онлайн-покупках через фишинговые ссылки

- *Ситуация: на сайтах, где торгуют частные продавцы, можно встретить мошеннические схемы. Злоумышленники размещают фейковые объявления и просят покупателей перейти на общение в мессенджере. Когда покупатель уточнил все детали сделки, собеседник отправляет ссылку на сайт, очень похожий на сайт платежной системы. Покупатель вводит данные карты, и мошенники крадут его деньги.*

Ваши действия в данной ситуации

- *Не переходить на общение с продавцом в мессенджере. Если все же перешли, проверять сайт и ссылку. Дизайн сайта должен быть аккуратным, а все разделы — кликабельными. В написании ссылки не должно быть ошибок, начинаться она должна с https://, а на адресной строке должен быть значок закрытого замка: это значит, что соединение безопасно.*

БС Банк

Мошенничество через СМС и электронные письма

- *Ситуация: злоумышленники отправляют СМС, письмо на почту или сообщение в мессенджер якобы от банка, госорганизации, известного бренда или благотворительного фонда. В сообщении просят перейти по ссылке, чтобы получить выигрыш или узнать о штрафе. Если это сделать, вредоносная программа скачивается на устройство и крадет данные — так мошенники получают удаленный доступ к вашему телефону или онлайн-банку.*

Ваши действия в данной ситуации

- *Не открывайте письма и сообщения, в которых вам обещают большую выгоду вроде выигрыша или легкого заработка. Не переходите по подозрительным ссылкам. Мошенники могут использовать подмену номера, поэтому всегда внимательно проверяйте ссылки даже в СМС, пришедших с номера вашего банка.*

Какими данными можно делиться, а какими нельзя

Чем безопасно делиться

Чаще всего данные карты нужно сообщить кому-либо, чтобы перевести деньги. Для перевода через Систему быстрых платежей достаточно номера телефона и названия банка, которым вы пользуетесь. Но бывают случаи, когда удобнее перевести так:

- *по номеру банковской карты — он состоит из 16 цифр и расположен на лицевой стороне. Из того, что написано на карте, сообщить можно только его.*
- *по номеру расчетного счета из 20 цифр, к которому привязана карта. Обычно этот номер запрашивают организации, чтобы оплатить ваши услуги. Возможно, им также понадобится БИК и корреспондентский счет — это реквизиты банка, их тоже можно сообщать без опаски. Номер расчетного счета можно посмотреть в приложении банка.*

Что нельзя говорить никому

Некоторые данные карты должен знать только ее владелец:

- *коды из СМС от банка: получив код, мошенник может подтвердить покупку или оформить кредит*
- *трехзначный код с оборотной стороны карты: с его помощью можно оплатить практически что угодно*
- *ПИН-код: с ним злоумышленник сможет снять деньги, даже не имея на руках карты*
- *срок действия карты: в редких случаях мошенник может совершить покупку, зная лишь ваше имя, номер карты и дату ее выпуска*

БС Банк

Общие правила финансово-цифровой гигиены

Вот несколько простых действий, которые помогут защитить ваши деньги от злоумышленников:

- *Пользуйтесь определителем номера. Можно скачать отдельное приложение или включить опцию определителя в приложении банка, если она есть. Если позвонят с подозрительного номера, он покажет сообщение «Возможно, это мошенники» — вы сможете не брать трубку*
- *Подключите двухфакторную систему аутентификации в банковском приложении. С ней мошенникам для входа в личный кабинет понадобится не только пароль, но и код из СМС*
- *Поставьте антивирус на все устройства. И на телефон тоже. Он не пропустит спам и защитит от вирусов, которые могут украсть персональные данные*
- *Установите лимит по карте. Даже если мошенники получат доступ к счету, с еженедельным или ежемесячным ограничением трат украсть все деньги не получится*
- *Заведите дополнительную карту для покупок в интернете с отдельным счетом. Даже если вы случайно перейдете по вредоносной ссылке или сообщите кому-то данные этой карты, потери будут менее ощутимы*

БС Банк