

Новое мошенничество в финансовой сфере



Специалисты Центра по информированию и консультированию потребителей ФБУЗ «Центра гигиены и эпидемиологии в Новгородской области» обращают внимание граждан, что злоумышленники теперь используют не только копии паспортов при оформлении «фейкового» кредита, но и взлом банковских приложений, а также прибегают к хакерским уловкам нового поколения.

Схемы мошенников

Схема № 1. Мошенники оформляют кредиты на россиян при помощи паспортов других людей — об этом давно и всем уже известно. Эта схема мошенников, в которой используются «слитые» паспортные данные, сегодня уходит в прошлое — документы в финансовых организациях стали проверять значительно лучше и качественнее, чем 10–15 лет назад.

Схема № 2. Между тем вторая широко распространённая схема для оформления мошеннических кредитов, а также кредитных карт связана с онлайн-банками. Такой сценарий очень популярен и в ближайшие годы он будет только развиваться ещё больше. Для этой схемы злоумышленникам необходимо получить доступ к вашему мобильному или онлайн-банку. Мошенники используют установку программ удаленного доступа на смартфон, фишинговые атаки и др. Цель их проста: получить коды из SMS и подключиться к аккаунту в онлайн-банке. Для выяснения кодов из SMS в игру нередко вступают телефонные мошенники, которые притворяются разными людьми — к примеру, сотрудниками служб безопасности банков или правоохранительных органов, а затем обманом узнают у жертв необходимую информацию.

Эта схема применяется ко всем, кто использует онлайн-банкинг, её география охватывает всю страну. Чаще всего мошенники, которые пытаются оформить кредиты на своих жертв, действуют в больших городах. И это объясняется следующим: в крупных городах больше потенциальных жертв, а постоянные потоки людей предполагают меньшее количество времени на проверку тех или иных данных в финансовых учреждениях. Местные правоохранительные органы сильно перегружены, поэтому мошенники получают благоприятные условия для совершения преступлений. В зоне риска, как правило, — население трудоспособного возраста и пенсионеры. Главным образом это связано с критериями выдачи кредитов и займов, в том числе минимальным и предельным возрастом заёмщиков.

Схема № 3. Злоумышленники прибегают к хакерским уловкам нового поколения и это самый новый вид мошенничества в финансовой сфере, а именно: к помощи искусственного интеллекта. А заключается он в следующем. В мессенджерах от вашего друга/подруги/знакомца рассылаются аудиосообщения в адрес всех ваших друзей/знакомых с просьбой перевести деньги, при этом голос и манера разговора полностью копирует голос и манеру разговора вашего друга (сгенерирован искусственным интеллектом). Соответственно у вас даже и мысли не возникает о том, что это может быть мошенник и вы уже готовы помочь своему другу всем, чем только можете и так быстро, как он просит в своём сообщении.



Общие правила. Защита.

Специалисты Центра отмечают: чтобы избежать оформления кредитов со стороны мошенников, очень важно проверять свою кредитную историю. Любой человек может узнать о своей задолженности перед финансовыми организациями путём запроса «Сведения бюро кредитных историй» на сайте «Госуслуги» или при помощи сайта Банка России. В том случае, если кредитор уже обратился в суд и тот принял решение не в вашу пользу, узнать об исполнительных производствах и взысканиях можно на сайте ФССП России по ФИО и дате рождения.

Помимо этого, советуем следить за кредитной историей в соответствующих бюро, например, Национальном бюро кредитных историй (НБКИ) и Объединённом кредитном бюро (ОКБ). Бесплатно запрашивать свою историю гражданин может дважды в год. В бюро хранится

вся информация по займам и кредитам, а также по действующим просрочкам и задолженностям. Если же человек уже стал жертвой мошенников, то советуем, как можно быстрее истребовать максимальный объем информации об организации-кредиторе, а также о том, с какого номера телефона злоумышленники звонили в кредитную или микро финансовую организацию. Данную информацию необходимо приложить к подробному заявлению о преступлении в правоохранительные органы, в котором следует детально изложить все доводы, обстоятельства и описать подтверждающие факты. С заявлением о возбуждении уголовного дела по ст. 159 «Мошенничество» УК РФ вам будет намного проще опротестовать взятый на вас кредит. В дальнейшем всё зависит от того, каким именно способом злоумышленники оформляли заем.

При схеме с использованием «слитых» паспортных данных потерпевшему легче всего опротестовать взятый кредит. Достаточно провести графологическую экспертизу подписей и доказать, что вас в этот день не было в локации, где был оформлен заем. Судебная практика по таким случаям обширна, и вероятность успешного исхода высока. Дело в том, что микро-финансовая организация выдаёт денежные средства по договору потребительского займа в соответствии с ФЗ-151. Такие соглашения признаются реальной сделкой и считаются заключёнными сразу после передачи денег заёмщику. Так, если потребитель лично не заключал договор и деньги от кредитора не получал, то у займодавца нет оснований требовать от него возврат займа, взятого третьим лицом без ведома потерпевшего.

В том случае, если злоумышленники использовали онлайн-банкинг, опротестовать такой кредит будет сложнее и дольше — потребуется сбор технической информации, а также данных биллинга (от англ. bill – счет) – система контроля оплаты услуг. Придётся доказывать, что ваш аккаунт был взломан, а вы стали жертвой обмана.

Чтобы не оказаться в подобной неприятной ситуации, специалисты Центра советуют соблюдать несколько простых правил безопасности:

1) рекомендуем всегда учитывать, что далеко не все коммерческие организации добросовестно относятся к вопросам сохранности личных данных своих клиентов. Поэтому следует как можно реже оставлять копии своего паспорта где бы то ни было, если в этом нет острой необходимости;

2) для входа в приложения онлайн-банкинга нужно устанавливать надежные пароли, а также доступ по отпечаткам пальцев или при помощи Face ID. Необходимо помнить, что сегодня оформление кредита в банковском приложении — это вопрос всего пары кликов;

3) регулярно проверять состояние своих счетов в тех банках, где они открыты. Если вы не пользуетесь услугами какого-либо банка, лучше всего закрыть там все счета;

4) при получении от «друга» в мессенджере аудиосообщения с просьбой перевода денег, в первую очередь перезвонить другу по мобильному телефону, а не переводить запрашиваемые мошенниками денежные средства на их счёт.

По вопросам соблюдения требований законодательства о защите прав потребителей можно обращаться:

- в Управление Роспотребнадзора по Новгородской области по адресу: В. Новгород, ул. Германа, д.14, тел.971-093; 971-095;

- в Центр по информированию и консультированию потребителей по адресу: г. Великий Новгород, ул. Германа 29а, тел. 77-20-38, 73-06-77;

- в отдел МФЦ по г. Великому Новгороду (адрес: 173000, г. Великий Новгород, ул. Большая Московская, д. 24) консультации можно получить каждый первый четверг месяца с 10-00 до 17-00.

Работает Единый консультационный центр, который функционирует в круглосуточном режиме, по телефону 8 800 555 49 43 (звонок бесплатный), без выходных дней на русском и английском языках.

Дополнительно информируем, что функционирует Государственный информационный ресурс для потребителей <https://zpp.rospotrebnadzor.ru>. Каждый потребитель может ознакомиться с многочисленными памятками, обучающими видеороликами, образцами претензионных и исковых заявлений. На ресурсе размещена вся информация о судебной практике Роспотребнадзора в сфере защиты прав потребителей.