Приднестровский республиканский банк

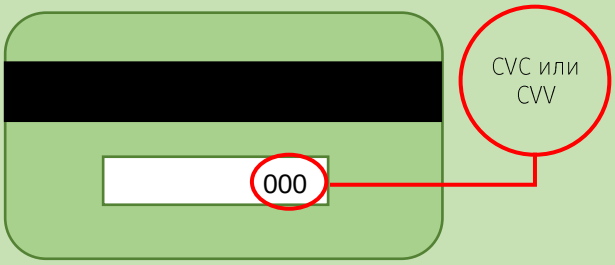
Как уберечь себя и близких от финансового мошенничества

Списание денег со счета без согласия владельца, похищение паролей и ПИН-кодов, подозрительно простой способ заработка в Интернете – все это разновидности финансового мошенничества. Мошенники могут сулить несметные богатства, маскироваться под служащих банков или представителей государственной власти, чтобы заполучить ваши деньги. Как распознать преступника и какими должны быть ваши действия, если вас обманули?

Попасть на удочку мошенника может каждый, и неважно, расплачивается он банковской картой или наличными. У аферистов существует множество способов заполучить ваши деньги: украсть деньги онлайн, с помощью телефонных звонков, СМС, сообщений в мессенджерах, социальных сетях и т.д. Как у них это получается?

Махинации с банковскими картами

Чтобы украсть деньги с вашей карты, грабителям нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV.



Номер CVC или CVV – это, как правило, последние три цифры, расположенные на оборотной стороне карты.

Мошенники могут установить, например, видеокамеру в банкомате. Если вы будете снимать деньги и не прикроете рукой клавиатуру в момент набора ПИН-кода, то ваши деньги могут с легкостью снять, перевести на другой счет и потом обналичить. Украсть данные вашей карты могут даже в обычном магазине. Преступником может оказаться продавец, который получит доступ к вашей карте хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в Интернете.

Как не попасться:

- При наборе ПИН-кода всегда закрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в супермаркете.
- Старайтесь всегда свою карту держать при себе.
- Подключите мобильный банк и СМС-уведомления.

Если совершаете покупки через Интернет, никому не сообщайте секретный код для подтверждения операций, который приходит через СМС.

Вас обокрали. Что делать?

✓ Позвоните в банк (номер есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.

✓ Запросите выписку по счету и напишите заявление об отмене операции.

✓ Оформите заявление в отдел милиции по месту жительства.

Вы потеряли карту

В таком случае нужно срочно заблокировать карту. Ведь велика вероятность, что мошенники в любую минуту могут расплатиться ею или снять наличные. Заблокировать банковскую карту можно разными способами:

✓ По телефону горячей линии. Универсальный способ. Номер для экстренной связи всегда указан на официальном сайте банка (лучше заранее сохранить номер горячей линии банка в мобильном телефоне, чтобы не разыскивать его в экстренном случае). Оператор службы поддержки попросит назвать паспортные данные, кодовое слово или СМС-код, который пришлет вам на телефон. После этого он заблокирует карту.

✓ Через мобильное приложение. Самый быстрый способ, если у вас есть доступ к Интернету, приложение уже установлено на вашем телефоне и в нем есть опция по блокировке карты.

✓ В Интернет-банке. Удобно, если у вас подключен Интернет-банк и рядом есть компьютер, планшет или смартфон с доступом в Интернет. В личном кабинет на сайте банка обычно есть опция «Заблокировать карту». Свое решение надо будет подтвердить кодом из СМС, которое банк вышлет на ваш номер.

✔ В отделении банка. Если вы находитесь рядом с офисом банка или потеряли телефон вместе с картой, пишите заявление о блокировке карты в отделении. Но для этого понадобится паспорт.

Даже после блокировки карты вы по-прежнему можете пользоваться деньгами на счете, к которому она была прикреплена. Снять наличные можно в отделении банка, предъявив паспорт. Сразу после блокировки карты вы можете оставить заявку на выпуск новой.

Кибермошенничество

Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не рассчитываетесь. Вдруг вам приходит СМС или уведомление от имени банка со ссылкой, просьбой перезвонить по неизвестному номеру или с извещением о том, что вы стали неожиданным счастливчиком и получили денежный подарок. Или представители банка связались с вами для уточнения ваших личных данных и номера ПИН-кода от карты.

Или вдруг приходит слезливая просьба от родственников или друзей в социальных сетях, с которыми приключилась беда (попали в ДТП, напали грабители и т.п.), о переводе небольшой суммы денег на их счет. В большинстве случаев вы столкнулись с мошенничеством в чистом виде. За ссылками, вероятнее всего, спрятались вирусы, на другом конце телефона – профессиональные мошенники, которые хотят выманить обманным путем необходимые данные, а по ту сторону экрана – аферисты, которые манипулируют вашими чувствами и слабостями.

Как не попасться:

- Никому не сообщайте личные данные, тем более пароли и коды! Служащим банка они не нужны, а преступники получат возможность украсть ваши деньги.
- Если вы получили известие о проблемах у родственников или друзей, обязательно свяжитесь с ними лично!
- Не храните данные карт на компьютере или в смартфоне!

- Не переходите по подозрительным ссылкам, не перезванивайте по неизвестным номерам! Даже если ссылка кажется безопасной, а телефон правильным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера перепроверяйте в официальных источниках.
- Всегда перепроверяйте информацию! Если вам сообщили о якобы полученном выигрыше или с вашей карты якобы случайно списали деньги и просят назвать свои данные, чтобы остановить операцию, завершите разговор и перезвоните в свой банк по номеру телефона, указанному на обратной стороне вашей карты.
- Если вам приходит СМС о зачислении средств (при этом сообщение похоже на привычное уведомление банка), а затем звонит якобы недотепа, который по ошибке перечислил вам деньги и просит вернуть, не спешите ничего возвращать. Скорее всего, по факту никакие деньги не приходили, СМС - не от вашего банка, а звонил вам аферист. Проверьте состояние вашего счета, просмотрите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.
- Если вам приходит сообщение «Подтвердите покупку» и код, а следом раздается звонок опять же от «невнимательного» человека, который просит продиктовать код по причине того, что ошибочно указал ваш номер телефона, ни в коем случае не делайте этого! Таким путем преступники пытаются выманить у вас код, чтобы списать деньги с вашего счета.
- Установите на компьютер себе и родным антивирус.

Не стоит забывать, что повышение финансовой грамотности – один из главных способов противостояния мошенникам!

При подготовке статьи были использованы материалы сайта Финансовая культура.