ПЕРЕОФОРМЛЕНИЕ ВКЛАДА

Отмечен рост интереса мошенников к депозитам и банковским счетам граждан. Преступники связываются с гражданами, заинтересованными в переоформлении вклада на более выгодных условиях, после чего высылают им ссылку, сообщая, что она ведёт в интернет-банк. Жертвы вводят свои логин и пароль.

После этого возможны два сценария: вкладчики переводят деньги якобы на новый вклад, однако так и не получают к нему доступ, либо же злоумышленники, обладая данным для входа в интернет-банк жертвы, выводят оттуда все деньги.

ЗВОНКИ ОТ ЛИЦА ПРЕДСТАВИТЕЛЕЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Мошенники представляются сотрудниками МВД и уведомляют жертву о том, что в отношении её Банк России завел уголовное дело.

Обескураженный гражданин соглашается назвать злоумышленнику данные паспорта и банковской карты, что дает возможность преступнику вывести деньги со счета жертвы. Регулятор напоминает, что сообщать, кому бы то ни было, платёжные данные небезопасно.

СОВЕТЫ, КОТОРЫЕ ПОМОГУТ НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВЫХ МОШЕННИКОВ:

1. Не перечисляйте деньги на счета незнакомцев ни под каким предлогом. Мошенники могут сообщить о выигрыше в лотерею, о компенсации затрат, о возврате налогов и прочее. Однако для получения приза, например, необходимо перечислить определенную сумму;

2. Не переводите денежные средства на счета мобильных телефонов, на электронные кошельки. Причем даже в случае, если Вас просят сделать это при совершении покупки. Подавляющее число интернет-магазинов принимают оплату по факту доставки товара. Так лучше воспользоваться этим надежным способом расчета;

3. Не отправляйте ответных сообщений на незнакомые номера (особенно на короткие) и не перезванивайте. И, тем более, не отправляйте деньги ни на какие реквизиты, указанные в сообщении. Даже если оно написано от имени банка или госструктуры, лучше уточнить информацию, позвонив на официальный номер учреждения;

4. Приобретая товары с рук на условиях предоплаты, убедитесь в благонадежности продавца. Посмотрите отзывы, узнайте его рейтинг на площадке объявлений, да и в целом поищите какую-нибудь информацию в информационно-телекоммуникационной сети «Интернет»;

5. Не сообщайте никому данные своей банковской карточки. В особенности это касается кода CVC2 и CVV2, расположенного на оборотной стороне. Также не озвучивайте кодов из смс, отправляемых банком и, тем более, ни в коем случае не сообщайте никаких паролей;

6. Не переходите по ссылкам, присланным с незнакомых номеров.

КУДА МОЖНО ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ?

в правоохранительные органы по месту жительства;
в Службу по защите прав потребителей и обеспечению доступности финансовых услуг Банка России:
по адресу: 107016, г. Москва, ул. Неглинная, д. 12;
по электронной почте: fps@cbr.ru;
через Интернет-приемную на сайте в информационно-телекоммуникационной сети «Интернет» (www.cbr.ru) в разделе «Сервисы. Интернет-приемная»;
задать вопрос по телефону: 8-800-300-3000.

Государственный контракт от 12.05.2021 № 009-ЭА/2021
Тираж 100 000 экз.
Изготовитель: НАО «Печатный двор Кубани»

Материалы подготовлены в рамках реализации пункта 1.1.1 подпрограммы «Финансовое просвещение населения Краснодарского края» государственной программы Краснодарского края «Социально-экономическое и инновационное развитие Краснодарского края» (постановление главы администрации (губернатора) Краснодарского края от 5 октября 2015 года № 943).

Министерство экономики Краснодарского края

«Осторожно! Мошенничество на финансовом рынке»

Очень часто у человека уходит целая жизнь на то, чтобы накопить ту или иную сумму денежных средств, потерять же ее он может за считанные минуты. Одним из наиболее распространенных видов экономических преступлений является мошенничество на финансовых рынках.

«ФИНАНСОВЫЕ ПИРАМИДЫ»

Одно из самых распространенных видов мошенничества на финансовом ранке – создание «финансовых пирамид». Несмотря на отсутствие в российском законодательстве определения понятия «финансовая пирамида», Банк России выделяет следующие внешние признаки, свидетельствующие о том, что организация или группа физических лиц является «финансовой пирамидой»:

выплата денежных средств участникам из денежных средств, внесенных другими вкладчиками;

отсутствие лицензии ФКЦБ/ФСФР России или Банка России на осуществление деятельности по привлечению денежных средств;

обещание высокой доходности, в несколько раз превышающей рыночный уровень;

гарантирование доходности (что запрещено на рынке ценных бумаг);

массированная реклама в СМИ, в информационно-телекоммуникационной сети «Интернет» с обещанием высокой доходности;

отсутствие какой-либо информации о финансовом положении организации;

отсутствие собственных основных средств, других дорогостоящих активов;

нет точного определения деятельности организации.

КИБЕРМОШЕННИЧЕСТВО

Под кибермошенничеством понимают вид недобросовестных действий, реализуемых дистанционно. Основной целью участников подобных операций является хищение денег у физических и юридических лиц.

Яркие примеры таких правонарушений – завладение денежными средствами лжесубъектами, расположенными в информационно-телекоммуникационной сети «Интернет». Нередко мошенники создают сайты-дубликаты официальных ресурсов, принадлежащих добросовестным профессиональным участникам финансового рынка.

Воровать киберпреступники могут не только деньги, но и другие блага. Например, бонусы с карт лояльности. Взламывая личные кабинеты клиентов на популярных сервисах, мошенники пытаются списать бонусные баллы жертв для оплаты собственных покупок. Или же и вовсе регистрируют личный кабинет с привязанной к нему картой другого лица (жертвы мошенников).

Существую случаи получения онлайн-займов в интернете, путем предоставления заведомо недостоверных и (или) ложных сведений о заемщике. Не менее распространены преступные схемы, связанные с заключением договоров страхования в электронном виде.

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

В связи с активным ростом рынка электронных платежей и онлайн-шопинга развиваются и новые современные формы мошенничества с использованием информационных технологий. Самыми распространенными видами мошенничества в информационно-телекоммуникационной сети «Интернет» являются следующие махинации:

фишинг – кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты;

мошенничество через электронную почту – так называемые «нигерийские письма». Они содержат в себе красивую легенду о наследстве от мифического родственника и просьбу перевести деньги на счет для получения оплаты услуг адвоката или выплаты комиссии;

махинации с интернет-кошельками – чаще всего в таких случаях покупатель переводит предоплату продавцу на интернет-кошелек, но в итоге не получает ни товара, ни денег.

МОШЕННИЧЕСТВО ПО ТЕЛЕФОНУ

Мошенничество при помощи сотовой связи можно условно разделить на две группы. К первой следует отнести снятие денег непосредственно со счета владельца номера без его ведома. Такими махинациями могут заниматься как сами сотовые операторы, так и не имеющие отношения к их компаниям мошенники. Во вторую группу мошенничеств можно отнести случаи, в которых абонент сам перечисляет деньги на указанный счет, либо отдает их прямо в руки или оставляет в указанном мошенниками месте. В таких аферах сотовая связь выступает лишь в качестве инструмента инсценировки.

Например, разыгрывается звонок близкого родственника, попавшего в беду и срочно нуждающегося в деньгах. Аферы продумываются до мельчайших деталей и способны обмануть бдительность даже самых осторожных и внимательных людей.

Именно поэтому необходимо помнить о том, что персональные данные, такие, как пароль, логин, номер банковского счета, кодовое слово, CVV2-код на банковской карте нельзя передавать в третьи руки.

Любая попытка получить данные сведения должна настораживать и может являться поводом для обращения в соответствующие органы.

ПРОДАЖА В ДОЛГ

Мошенники покупают товары с рук, переводя средства на счета, принадлежащие продавцу (жертве), после чего забирают товар и отправляются по своим делам. Затем покупатель-мошенник обращается в суд с распечатанным счетом, который в суде могут приравнять к долговой расписке, и получает исполнительный лист. В итоге несуществующий долг могут списать с жертвы в пользу мошенника.