ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ЗЛОУМЫШЛЕННИКИ ВЫДАЮТ СЕБЯ ЗА СОТРУДНИКОВ БАНКА

Самые распространенные способы хищения средств с банковских карт основаны на психологических методах убеждения, обмана или запугивания граждан.

I. Мошенники выдают себя за сотрудников банка и сотрудников правоохранительных органов

Ситуация 1

Мошенники, представляясь по телефону банковскими сотрудниками (службой безопасности или службой финансового мониторинга), сообщают гражданину о подозрительной активности, зафиксированной по его счетам (банковским картам), и предлагают продиктовать данные карты, чтобы банк принял меры по защите средств.

Убеждают перевести деньги на отдельный счет якобы для их защиты, с которого впоследствии похищаются денежные средства.

Предлагают установить специальное программное обеспечение для «защиты средств».

Данные программы предоставляют мошенникам возможность удаленного доступа к телефону гражданина и последующего оформления кредита в приложении банка.

Ситуация 2

Гражданину звонят на телефон и мошенник, представившись сотрудником банка, сообщает ему о том, что от его имени была подана заявка на кредит. При этом гражданин отрицает оформление заявки, но преступник упорно продолжает настаивать, что заявка оформлена. Гражданин, испугавшись стать обладателем неожиданного кредита, вступает в доверительный разговор с мошенником о дальнейших действиях. Преступник предлагает потерпевшему пройти в офис банка и оформить кредит на его имя, а после получения кредита перевести его на безопасный счет.

Если гражданин соглашается, то в последствии этого - все денежные средства оказываются в распоряжении преступников.

Ситуация 3

Гражданину поступает звонок от якобы сотрудника (следователя) Следственного комитета России или сотрудника полиции, при этом лжесотрудник сообщает гражданину, что на его паспортные данные преступники пытались оформить кредит в банке и принимаются меры к их задержанию. Далее лжесотрудник говорит, что с гражданином свяжется сотрудник банка (также мнимый) по телефону и гражданину, будучи на связи с этим мнимым сотрудником банка, следует пройти в ближайший к нему офис банка. Когда гражданин оказывается в офисе банка, мнимый сотрудник банка, находящийся на связи по телефону, предлагает ему через банкомат оформить кредит, чтобы опередить преступника, пытавшегося оформить его на паспортные данные гражданина, и перевести этот кредит на безопасный счет - счет мошенников.

Ситуация 4

Гражданину звонят по телефону, мессенджеру «Вайбер», «Ватсап», представляются сотрудником банка, спрашивают, подавал ли он заявкуна смену номера телефона. Услышав отрицательный ответ, мошенник предлагает принять меры для безопасности счета гражданина и просит продиктовать номер телефона, к которому подключен мобильный банк. Гражданин диктует это номер телефона, а мошенник вводит этот номер в соответствующее приложение банка, гражданину приходит код, необходимый для входа в личный кабинет (для восстановления пароля), мошенник просит назвать его, получая при этом доступ к личному кабинету

ЧТО ДЕЛАТЬ?

- перепроверьте сообщенную вам информацию, прервав разговор, позвонив на «горячую линию» банка, полицию, родственникам;
- попросите, чтобы звонившие лжесотрудники банка или полиции полностью назвали ваши персональные данные и паспортные данные, либо данные родственника, попавшего в беду, поскольку настоящие сотрудники банка и полиции такими данными владеют;
- не скачивайте и не используйте «специальное» приложение, якобы необходимое для защиты персональных данных или отмены заявки на кредит;
- не отправляйте деньги на неизвестный банковский счет, помните, что настоящие сотрудники банка таких предложений (по переводу денежных средств на безопасные счета) не делают.

II. Фейковые СМС от банка, иные СМС и сообщения

* смс-сообщения на телефон о блокировке карты. Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки искусного мошенника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки;
* смс-сообщения с кодом для подтверждения покупки/иной операции, которую человек не совершал - далее поступает звонок от мнимого сотрудника банка с просьбой продиктовать код.

Все эти действия злоумышленников под различными мнимыми предлогами направлены на то, чтобы получить доступ к данным вашей банковской карты.

III. Мошенничество в сети Интернет при покупке театральных билетов

Возросло количество фальшивых сайтов по продаже билетов. Одна из самых распространённых схем мошенничества - продажа билетов через поддельные сайты, домен которых лишь немного отличается от официальной страницы сайта в сети Интернет того или иного театра. Через них мошенники продают билеты с большой наценкой и по несколько раз, отчего одно место в партере может быть куплено сразу двумя зрителями, либо куплены поддельные несуществующие) билеты.

Ситуация

В сети Интернет, в поисковой строке при поиске «купить билет» гражданин попадает на фейковый сайт по продаже билетов, например camedi, cassir.ru, где для покупки билета человеку предлагается зарегистрироваться и в последствии ввести реквизиты карты. При покупке билета на таком сайте денежные средства оказываются в распоряжении преступников, а гражданин получает фальшивые билеты.

ЧТО ДЕЛАТЬ?

Изучите сайт, на котором собираетесь делать покупку. Мошеннические ресурсы часто содержат гораздо меньше информации, чем настоящие сайты организаций культуры.

Обращайте внимание на адрес сайта, если в нем содержатся ошибки и опечатки - с высокой долей вероятности это поддельный ресурс. Если сайт размещен в иностранной доменной зоне, особенно редко встречающейся, например: .CO (Колумбия) или .KO (Румыния) - вероятнее всего ресурс поддельный.

С осторожностью относитесь к любой информации, которая заставляет вас торопиться с принятием решения. Ограниченные сроки или ограниченное количество товара - один из приемов, используемых мошенниками.

Внимательно проверяйте реквизиты организации, которой вы переводите оплату за покупку. Если вы покупаете билет на сайте театра (т.е. юридического лица), но при оплате видите то, что переводите деньги частному лицу или с карты на карту - есть основания подозревать, что это мошенники.

При любых вопросах относительно покупки билета звоните в кассу театра для уточнения информации, номера телефонов можно узнать в самом театре при личном визите, либо на официальном сайте в сети Интернет.

IV. «Ваш родственник попал в беду»

Мошенники действуют по сценарию «Ваш родственник попал в беду». Телефонные звонки часто совершаются ночью. Чтобы жертва не успела опомниться.

Подобными телефонными звонками аферистам чаще всего удается обмануть самую доверчивую часть населения - людей пожилого возраста.

Ситуация

Преступник звонит по телефону потерпевшему, представляясь его сыном (дочерью, внуком), которого задержали, и он как будто находится в полиции, просит о помощи. Далее в разговор с потерпевшим вступает лжесотрудник силового ведомства (полиция, прокуратура, следственный комитет), и подтверждает информацию о сложившейся ситуации, а также сообщает, что для разрешения возникшей ситуации необходимы деньги. По адресу потерпевшего приезжает курьер (нередко в качестве курьеров используют водителей такси), а потерпевший, думая, что помогает попавшему в беду родственнику, отдает деньги в руки мошенникам.

Обычно разговор длится недолго. Мошенник говорит тихо либо неразборчиво, чтобы потерпевший не мог точно определить по голосу, кто ему звонит, и с первых слов распознать обман.

ЧТО ДЕЛАТЬ?

При поступлении подобного звонка не нужно беседовать с неизвестным и впадать в панику.

Под любым предлогом прервите разговор и сами перезвоните родственнику, от имени которого звонят или о котором идет речь.

Если его телефон отключен, то перезвоните другим родственникам.

Позвонив в отдел полиции можно узнать, действительно ли родственник находится в полиции.

Поинтересуйтесь именем и должностью собеседника, на которого тот ссылается, и его личными данными.

Незамедлительно сообщите сотрудникам полиции о совершаемых в отношении вас мошеннических действиях.

V. Мошенничество при продаже товаров на сайтах объявлений «Авито», «Юла» и т.п.

Гражданин разместил объявление о продаже товара на сайтах «Авито», «Юла» и т.д.

Мошенники, предварительно узнав его номер телефона при непосредственном общении при звонке на защищенный на сайте номер телефона, отправляют гражданину в мессенджере сообщение со ссылкой на сервис «Авито - безопасная сделка». Однако она перенаправляет на созданный мошенниками сайт-двойник, открывающий им доступ к вашему личному кабинету в мобильном банке.

При переходе по ссылке, жертве предлагается ввести данные банковской карты якобы для получения денег за продаваемый товар, после чего на телефон приходит смс сообщение от банка с паролем, при вводе которого с банковской карты жертвы

ЧТО ДЕЛАТЬ?

Ни в коем случае не следует переходить по ссылкам, которые вам присылают незнакомцы.

Переписка с продавцом и оформление сделки должны проводиться только на официальном сайте онлайн объявлений.

В случае сомнения немедленно прервите беседу и обратитесь в службу технической поддержки сайта.

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

По телефону НЕЛЬЗЯ:

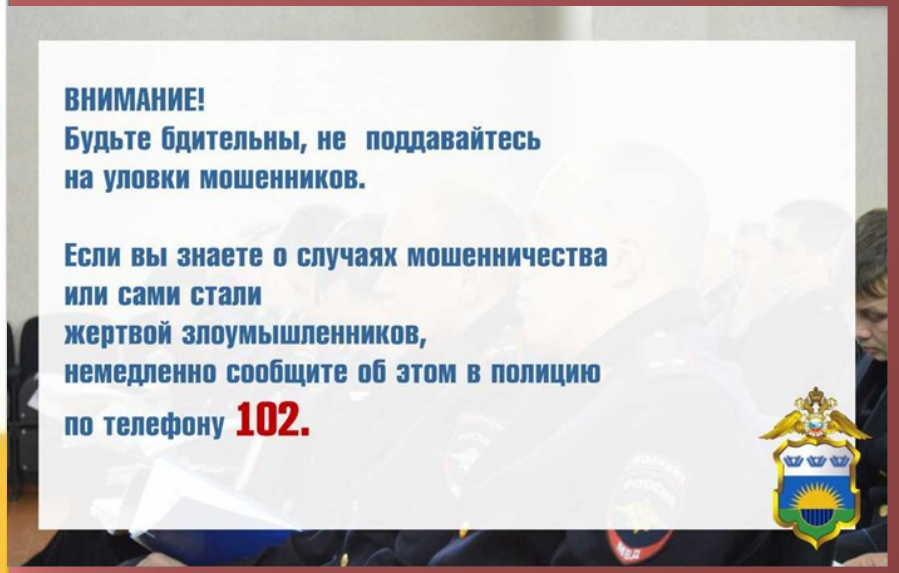
1. Выиграть миллион рублей

2. Спасти близкого человека, попавшего в беду

3. Разблокировать банковскую карту

4. Купить редкие товары и уникальные таблетки!

По телефону можно стать ЖЕРТВОЙ МОШЕННИКА!



УМВД России по Тюменской области
625000, г. Тюмень,
ул. Водопроводная, 38
тел. 8 (3452) 793-023
или 102 (для абонентов мобильной связи).