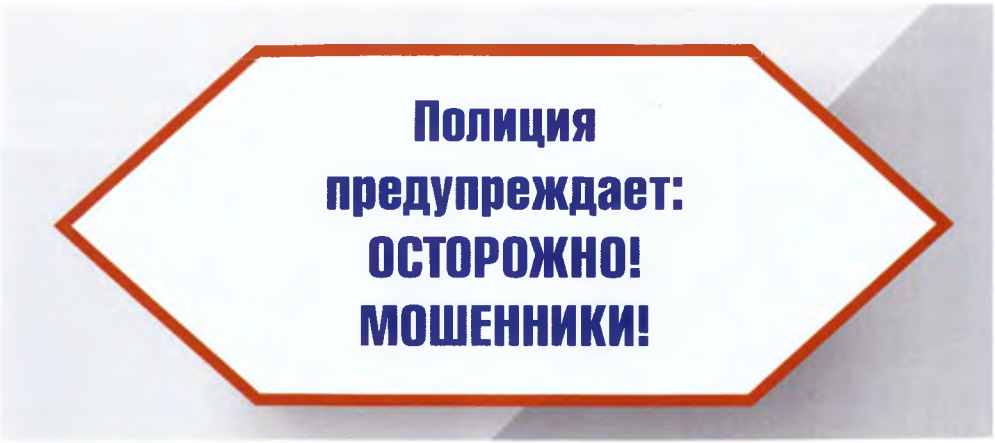
Совет при Тюменской
областной Думе
по повышению
правовой культуры
и юридической
грамотности населения
Тюменской области

Управление
МВД России
по Тюменской
области

ПАМЯТКА



ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ IT-ТЕХНОЛОГИЙ

г. Тюмень
2022 год

СХЕМЫ МОШЕННИЧЕСТВА

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

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

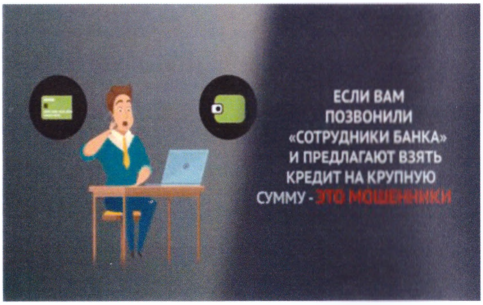
Мошенники, представляясь по телефону банковскими сотрудниками (службой безопасности или службой финансового мониторинга), сообщают гражданину о подозрительной активности, зафиксированной по его счетам (банковским картам), и предлагают продиктовать данные карты, чтобы банк принял меры по защите средств.

Убеждают перевести деньги на отдельный счет 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



Гражданину поступает звонок на телефон, и мошенник, представившись сотрудником банка, сообщает лицу о том, что от его имени была подана подозрительная заявка на кредит. При этом, чтобы не вызвать подозрения, мошенник не просит сообщить ни CVC-код, ни иные данные банковской карты.

Расположив к себе гражданина, мошенник предлагает ему войти в приложение банка и оформить заявку на кредит на ту же самую сумму, на которую мошенниками «якобы оформлена» заявка. Преступники сообщают лицу, что при оформлении им заявки через приложение, установленное непосредственно на его мобильном телефоне, поданная мошенниками заявка будет аннулирована. При оформлении заявки гражданином в мобильном приложении и ее одобрении банком преступники, находясь все это время на связи с лицом, начинают настаивать на переводе денежных средств на «специальный счет». Последствие этого – все денежные средства оказываются в распоряжении преступников.

Ситуация

Гражданину поступает звонок от лжесотрудника (лжеследователя) 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, находясь 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.

Что делать?

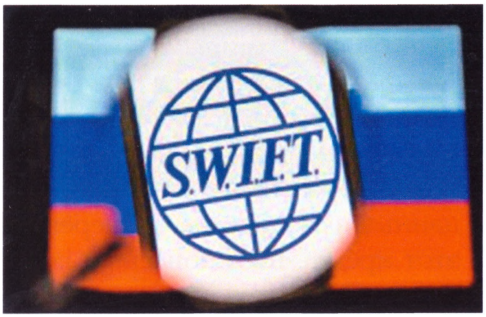
Перепроверьте сообщенную вам информацию, прервав разговор, позвонив на «горячую линию» банка или в полицию;

попросите, чтобы звонившие лжесотрудники банка или полиции полностью назвали ваши персональные данные и паспортные данные, поскольку настоящие сотрудники банка и полиции такими данными владеют;

не скачивайте и не используйте «специальное» приложение, которое предлагают установить 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 высказывают.

2. Отключение держателей банковских карт от международной системы SWIFT



Мошенники используют тему отключения российских банков от SWIFT (канал для обмена финансовой информацией, в том числе платежными поручениями, подтверждениями сделок и другой документацией). Гражданам предлагают перевести их сбережения на «безопасные счета».

Ситуация

Мошенники, представившись сотрудниками банка, звонят гражданам, являющимся держателями банковских карт и «объясняют», что после отключения России от SWIFT граждане потеряют все свои накопления. Для спасения средств необходимо срочно совершить перевод в другой банк или на специальный «защищенный» счет, который уже подготовлен «сотрудником».

Что делать?

При малейших подозрениях гражданину следует немедленно прервать разговор и самостоятельно перезвонить по номеру, указанному на обратной стороне банковской карты.

Помните, что ни сотрудники банков, ни сотрудники полиции не обзванивают людей с целью рассказать о проблемах с платежными системами.

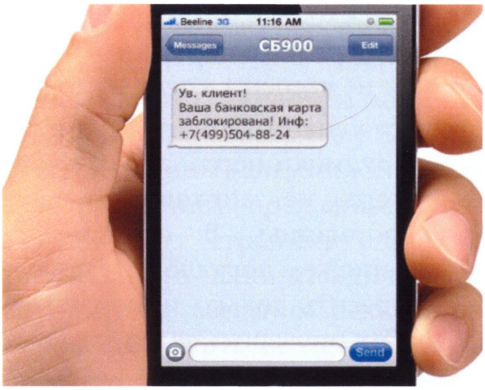
3. Фейковые СМС от банка, иные СМС и сообщения

* 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 лжесотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки искусного мошенника, выполняя его просьбы, и, сам того не замечая, передает свои конфиденци-

альные 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.



* Мошенник присылает гражданину посредством мессенджеров «Вайбер», «Вотсап», «Телеграм» сообщение о том, что для него истекает срок получения денежной компенсации, а для ее получения необходимо перейти по ссылке и указан адрес ссылки – **это также уловка мошенников, поддавшись на нее и перейдя по ссылке, вы можете лишиться денежных средств.**

Что делать?

Не переходите по ссылке, заблокируйте или удалите сообщение, никогда и никому не сообщайте свои данные, а также любую банковскую информацию.

4. Мошенничество на ГОСУСЛУГАХ

Злоумышленники представляются сотрудниками портала «Госуслуги». Свой звонок от имени службы поддержки портала «Госуслуги» мошенники объясняют либо утечкой данных, либо информацией об оформленном на имя гражданина кредите. Под этим предлогом злоумышленники пытаются выманить поступающий через СМС код сброса пароля к сервису, передача которого обеспечит, с их слов, «безопасность аккаунта».

Ситуация

Предварительно узнав номер мобильного телефона гражданина на сайтах бесплатных объявлений («Авито», «Юла»), мошенник сделал запрос на портале «Госуслуги» на восстановление аккаунта. Затем, позвонив гражданину и представившись работником службы технической поддержки портала «Госуслуги», поинтересовался: не сменил ли гражданин номер телефона. Мошенник, в целях введения в заблуждение гражданина, продиктовал любой номер и предложил для восстановления старого номера прислать на его номер еще один пароль.

Убедившись в корректности номера мобильного телефона, мошенник зашел на портал «Госуслуги», нажал на ссылку «Восстановить доступ по номеру» и вставил номер телефона гражданина. На номер телефона гражданина пришло смс с паролем. Гражданин продиктовал пароль, и мошенники получили доступ к аккаунту.

Что делать?

Чтобы обезопасить себя, достаточно соблюдать несколько простых правил:

- не переходите по ссылкам из смс-сообщений и электронных писем, если не уверены в отправителе;
- не сообщайте код из смс никому. Сотрудники портала «Госуслуги» никогда не запрашивают такую информацию. В официальной переписке с порталом у вас могут попросить только номер заявки, чтобы проверить её статус;
- доверяйте только официальной информации. Вы можете получить полную информацию на официальном портале «Госуслуги», по номеру телефона службы поддержки 8 800 100-70-10; официальный номер, с которого приходят СМС: 0919.

5. Мошенничество в сети Интернет

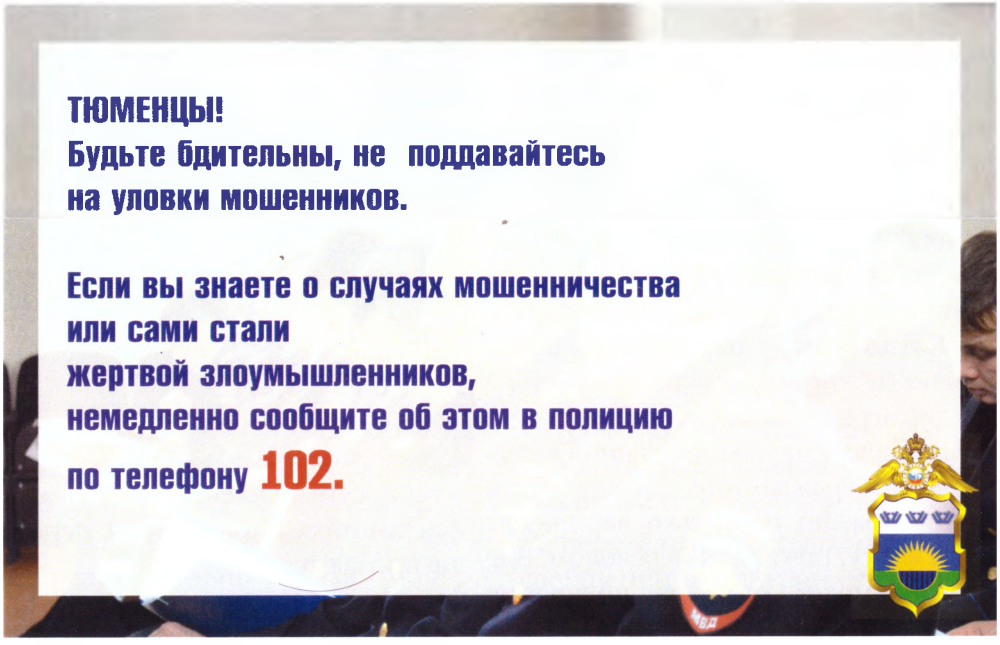
На разных сайтах появляется окно, что вам выпал приз и предлагается перейти по ссылке. При переходе по ссылке предлагается участие в лотерее путем открытия, например, коробочек с призами. При открытии первых двух выпадает пусто, а при открытии третьей – выигрыш на определенную сумму. Далее с целью получения выигрыша гражданину может быть предложено несколько вариантов: на карту, почтовым переводом. Вне зависимости от типа получения выигрыша от гражданина потребуется номер банковской карты и перевод пошлины или комиссии. Далее гражданину предлагается перейти на страницу оплаты (неизвестного платежного агрегатора) путем введения реквизитов банковской карты, в том числе защитного CVC-кода. При заполнении реквизитов банковской карты происходит автоматическое списание «пошлины» и ваши данные доступны для мошенников.

Что делать?

Получив сообщение о неожиданном выигрыше, нужно сразу насторожиться. Вы только что зашли в Интернет, и сразу же появилось объявление о розыгрыше, в котором вы не принимали участия.

Помните, что при реальном проведении конкурса, лотереи организатором сразу может быть вычтена сумма налога, подлежащая удержанию. Комиссии за перевод не взимаются.

Не вводите данные банковской карты, не производите оплату. В случае, если вы оплатили «пошлину» путем внесения реквизитов банковской карты через платежную систему, принадлежащую преступникам, переведите денежные средства на другой, принадлежащий вам счет и заблокируйте карту, чтобы преступники в дальнейшем не смогли воспользоваться средствами вашей карты.



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