КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Прекратите разговор.

Самостоятельно позвоните в банк.

(ваше реал номер телефона указан на банковской карточке)

1

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Не сообщайте свои персональные данные, а также:

- коды из смс;
- трехзначный код на оборотной стороне карты (CVV/CVC);
- PIN-код;
- пароли/логины к банковскому приложению и онлайн-банку;
- кодовое слово.

2

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Не надо сразу выполнять рекомендации, которые дает лицо, представляющееся сотрудником банка.

(вас торопят? задумайтесь!)

3

ВАЖНО ЗНАТЬ:

Настоящий сотрудник банка обладает всеми необходимыми ему сведениями о вас и ваших счетах.

Никаких „безопасных счетов", о которых говорят лица, представляющиеся сотрудниками банка, не существует.

Для того, чтобы „обезопасить средства" - глупо брать кредиты!

4

КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ

СОТРУДНИКАМИ БАНКА

СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ»:

В первую очередь, уточните полные данные лица, представляющегося сотрудником „правоохранительных органов", а также причину звонка.

Прекратите разговор.

1

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ»:

Позвоните в полицию и сообщите о странном звонке.

2

ВАЖНО ЗНАТЬ:

Настоящие сотрудники правоохранительных органов не привлекают граждан к содействию путем телефонных звонков или по видеосвязи.

3

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо – повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Как защитить свои финансы, читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ

Основные виды и способы совершения наиболее распространенных мошенничеств

1. Мошенничество на сайтах бесплатных объявлений (Авито, Юла и др.)

1.1. Покупка товара у потенциального потерпевшего.

Злоумышленник вступает в коммуникацию с потерпевшим посредством телефонной связи через официальное приложение, где в ходе разговора выражает готовность купить понравившийся товар. Для оплаты покупки он предлагает продиктовать ему номер банковской карты и остальные ее реквизиты. После получения необходимой информации злоумышленник предлагает продиктовать одноразовый пароль, который приходит на телефон жертвы. Данный пароль является разновидностью цифровой подписи и, продиктовав его, потерпевший сам подтверждает перевод со счета своей банковской карты или дает доступ к своему личному кабинету в приложении по предоставлению банковских услуг;

1.2. Продажа товара потенциальному потерпевшему.

Злоумышленник размещает объявление о продаже какого-либо товара на сайте бесплатных объявлений. Характерной чертой данных объявлений является заниженная относительно рыночной цена товара, а также удаленность продавца от районного центра. При обращении по объявлению потенциального потерпевшего злоумышленник может предложить внести предоплату под предлогом бронирования товара, на который имеется высокий спрос, на счет банковской карты или оформить доставку товара через услугу «Безопасная сделка». Для этого злоумышленник предлагает перейти для более удобного общения в один из популярных мессенджеров. Там в ходе общения злоумышленник может переслать фотографии и даже видеозаписи с демонстрацией работы продаваемого товара, после чего предоставляет фишинговую ссылку, якобы для оформления доставки. Перейдя по данной ссылке потерпевшему на сайте стилистически похожем на выбранную им службу доставки, предлагается заполнить форму, которая содержит его персональные данные, адрес, а также реквизиты банковской карты, после ввода которых последнему приходит одноразовый пароль для подтверждения операции списания. После ввода пароля у потерпевшего списываются деньги со счета банковской карты, реквизиты которой он ввел ранее.

2. Фейк-босс.

Потенциальному потерпевшему в одном из популярных мессенджеров приходит сообщение, якобы, от его руководителя с информацией о том, что с ним в скором времени свяжется куратор из ФСБ или другого силового ведомства, инструкции которого нужно будет выполнить беспрекословно. При этом стоит отметить, что аватар учетной записи может содержать реальный номер руководителя, а также его фотографию. После получения обратной связи, потерпевшему звонит злоумышленник, через один из популярных мессенджеров. Логотип аватара как правило также содержит официальную символику органа исполнительной власти или банковской организации. В ходе беседы потерпевшему предлагается принять участие в проведении мероприятий по выявлению сотрудников его организации, которые сотрудничают с вражеским государством, для чего необходимо осуществлять контрольные закупки с использованием как личных, так и кредитных денежных средств. Переводы денежных средств осуществляются на счета банковских карт и абонентских номеров. В исключительных случаях потерпевшему предлагается продать недвижимое и дорогостоящее движимое имущество.

3. Сотрудник банка.

Потенциальному потерпевшему осуществляется звонок, через один из популярных мессенджеров. Логотип аватара как правило также содержит официальную символику органа исполнительной власти или банковской организации. В ходе беседы потерпевшему предлагается принять участие в проведении мероприятий по выявлению сотрудников банка, которые занимаются

мошенническими действиями и пытаются похитить деньги потерпевшего. Для их изобличения необходимо осуществлять контрольные закупки с использованием как личных, так и кредитных денежных средств. Переводы денежных средств осуществляются на счета банковских карт и абонентских номеров. В исключительных случаях потерпевшему предлагается продать недвижимое и дорогостоящее движимое имущество.

При осуществлении вызова со стороны «сотрудников банка» злоумышленник будет рассказывать, что от имени клиента зарегистрирована заявка на смену доверенного номера или на оформление кредита. В случае МВД – собеседника могут обвинить в совершаемом им преступлении из-за переводов денежных средств в недружественные страны. «Специалисты» банка России будут убеждать собеседника срочно застраховать «единый лицевой счет» и иные счета, находящиеся в собственности клиента, а также осуществить перевод денежных средств на «безопасные счета».

4. Помощь родственнику, совершившему ДТП.

При звонкам пожилым гражданам злоумышленники представляются их родственниками и под предлогом совершения ими дорожно – транспортного происшествия, похищают денежные средства, за которыми как правило приезжают «курьеры», которые могут представляться помощниками следователей и сотрудников прокуратуры. Другие злоумышленники могут осуществлять звонки и предлагать вкладывать денежные средства путем инвестирования в различные акции компаний и предприятий, таких как ПАО «Газпром», АО «Тинькофф банк», а также принять участие в покупке различной иностранной валюты, в том числе цифровой, на иностранных биржах и иных торговых площадках.

Имеются простые способы, которые помогут защититься от преступных посягательства данного вида:

1. Не передавайте незнакомцам, звонящим в мессенджерах, конфиденциальную информацию (данные банковских карт, коды из СМС, логин и пароль для входа в личный кабинет)

2. Прекратите разговор, если позвонивший незнакомец под каким – либо предлогом убеждает осуществить перевод денежных средств куда – либо. Безопасных счетов и страховых ячеек не существует.

3. Чтобы снизить вероятность осуществления звонков от мошенников, в настройках телефона и в мессенджерах запретите незнакомым абонентским номерам осуществление входящего вызова, это также поможет пожилым родственникам.

4. Ни при каких обстоятельствах не устанавливайте незнакомое программное обеспечение на персональные компьютеры, а также на мобильные устройства, если не знаете принцип его работы.

5. Не соглашайтесь на предложения, поступившие посредствам мобильной связи, а также через мессенджеры и иные коммуникаторы (Скайп, Дискорт и т.д.) на участие в инвестировании различных компаний и предприятий. Не создавайте личных кабинетов на биржевых и торговых площадках дистанционно.

Стоит запомнить, что сотрудники банковских организаций и Центрально банка Российской Федерации никогда не осуществляют телефонных звонков гражданам с информацией о том, что с их счетов пытаются похитить денежные средства. Сотрудники полиции никогда не осуществляют звонки гражданам с предложением об участии в каких – либо следственных действиях по выявлению мошенников, а также по доведению информации для граждан о том, что их банковские счета могут подвергаться преступным посягательствам со стороны третьих лиц.

УУР УМВД