Лекция

по профилактике преступлений в сфере информационно-телекоммуникационных технологий

На территории Красноярского края правоохранительными органами все чаще регистрируются факты совершения хищений денежных средств с лицевых счетов граждан с использованием современных информационно-телекоммуникационных технологий. Потерпевшими становятся жители региона различных возрастных групп. Преступники при совершении хищений постоянно совершенствуются, придумывая новые способы, при этом активно используют Интернет-ресурсы, торговые площадки, возможности цифровой телефонии. Чтобы не попасть на уловки мошенников необходимо каждому знать, каким образом совершаются преступления и что ни в коем случае не стоит делать.

Как себя вести если Вам позвонил неизвестный и, представившись сотрудником кредитно-финансового учреждения, требует персональные данные Вашей банковской карты? Как обезопасить себя при совершении покупок либо продаж товара через Интернет? На сегодняшний день наиболее часто встречаются следующие способы совершения дистанционных хищений:

1. Хищение совершено с использованием средств IP-телефонии и телефонов сотовых операторов под предлогом предотвращения несанкционированного списания денежных средств, оформления кредита, блокировки банковской карты, сохранения денежных средств на «резервном» счёте. Преступник вводит жертву в заблуждение с помощью методов так называемой «социальной инженерии», получая реквизиты банковской карты и одноразовые коды в СМС, созданные для идентификации лица в системе дистанционного банковского обслуживания, как владельца, либо заставляет потерпевшего установить программы удалённого доступа «Team - Viewer» или «AnyDesk», распоряжается имеющимися на лицевом счёте денежными средствами, как правило переводя их на подконтрольные счета, используя различные платежные сервисы, электронные кошельки и номера телефонов операторов сотовой связи. В данном случае необходимо немедленно прекратить разговор, позвонить по номеру «горячей линии» банковского учреждения, в котором оформлена Ваша банковская карта, либо лично посетить офис банка и поинтересоваться по поводу сомнительных переводов.

Запомните! Сотрудники банка никогда по телефону не будут спрашивать персональные данные банковских карт, тем более код из СМС. Не существует такого вида сохранения средств, как внесение

наличности через терминал на «резервный» счёт либо перевод на абонентский номер. Ни в коем случае не передавайте персональные данные своей банковской карты, не устанавливайте в своем смартфоне либо компьютере какие-либо программы по просьбе неизвестного лица.

2. Хищение совершено посредством телефонного звонка под видом покупателя либо продавца по размещённому объявлению на торговых площадках сайтов «Авито», «Юла» и т.п. Преступник вводит жертву в заблуждение, поясняя, что в связи с нахождением за пределами Красноярского края, лично передать деньги не может и предлагает осуществить сделку дистанционно. Для этого, как правило, лица переходят для общения в мессенджеры, чаще «WhatsApp», договариваются о получении (отправке) товара с помощью служб доставки (Avito – доставка, CDEK, Boxberry и т.п.), преступники скидывают интернет – ссылку на фишинговые (поддельные) сайты, где жертва вносит реквизиты банковской карты.

Запомните! Торговые площадки оснащены системой защиты от сомнительных операций по переводу средств, позволяющей блокировать различные ссылки, поэтому если Вас покупатель/продавец просит перейти к общению в мессенджере и кидает ссылку, то это первый тревожный сигнал к тому, что Вас хотят обмануть. Зачастую ссылки, отправляемые преступниками, по названию могут быть схожи с названиями различных компаний по доставкам товара, даже с названиями самих торговых площадок. Не переходите по ссылкам, отправленным неизвестными лицами.

3. Хищение совершено посредством телефонного звонка под предлогом выдачи кредитов (займов). В данной ситуации, до совершения преступления, потерпевший самостоятельно находит предложения в интернет среде о предоставлении кредита, перейдя на «фишинговый» сайт, оставляет свои контакты. Злоумышленник, под видом работника кредитного учреждения, связывается с жертвой, выманивает реквизиты карты под предлогом оплаты комиссии и распоряжается деньгами через подконтрольные банковские счета. В данном случае надо знать, что, ведя переговоры по телефону по поводу доставки кредитных денежных средств и заранее оплачивая услуги курьера, сумму за страхование и открытие счёта, без документального подтверждения, Вы рискуете остаться без денег.

Самый надёжный способ получения кредита – это личное посещение банка.

4. Хищение совершено с использованием «фишинговых сайтов» в сети Интернет. Как правило, это «двойники» сайтов продаж авиабилетов, сайтов интернет - магазинов бытовой техники, электрооборудования и

электроинструментов. Различаться такие сайты от настоящих могут в одну букву или цифру. Домены таких сайтов обычно зарегистрированы за пределами Российской Федерации.

Необходимо помнить и знать, что самый надёжный способ приобретения билетов – это касса аэропорта, железнодорожного транспорта. Если же Вы решили купить билет в сети Интернет, то необходимо внимательно изучить сайт, почитать отзывы.

5. Хищение совершено с использованием сети Интернет в социальных сетях («Одноклассники», «ВКонтакте», «Инстаграмм»), в том числе путём взлома страниц. В этой ситуации прослеживается закономерность: в «Одноклассниках» жертвами становятся лица пожилого возраста, предлогом является мнимая выплата всякого рода компенсаций (НДС, доплаты к пенсии и т.п.). Во «Вконтакте» злоумышленником взламывается страница связей потерпевшего и от их имени, путём переписки, запрашиваются денежные средства в долг, с указанием реквизитов банковской карты. В социальной сети «Инстаграмм» распространены так называемые интернет – страницы продаж вещей, где под видом сделки преступники завладевают реквизитами банковских карт либо вынуждают внести предоплату за товар и не исполняют своих обязательств.

Если Ваш знакомый в социальной сети просит деньги в долг, необходимо связаться с ним по телефону, либо убедиться в ходе переписки, что с Вами общается именно он, а не мошенник, у которого в пользовании находится взломанная страница знакомого.

6. Хищение совершено посредством телефонного звонка, под предлогом освобождения родственника от уголовной ответственности. Преступники звонят, как правило, на домашние телефоны, представляются сотрудниками правоохранительных органов, доводят ложную информацию о том, что родственник собеседника якобы попал в беду (ДТП, сбил человека, избил кого-либо и т.п.). В данном случае преступники предлагают решить вопрос, для чего требуется определенная сумма денег, которую в последующем забирают через таксистов, либо предлагают зачислить денежные средства на банковские реквизиты.

Будьте внимательны! При поступлении подобных звонков, несмотря на уговоры преступников о том, что не стоит звонить никому, немедленно свяжитесь с родственником, который попал в «беду». В разговоре сохраняйте спокойствие и не называйте данные родственника, скажите неизвестному, что будете по данному факту обращаться в правоохранительные органы.

7. Хищение совершено под видом предоставления различных услуг, например по оформлению документов для трудоустройства. Данные преступления совершаются в результате размещения на интернет-сайтах по предоставлению услуг объявлений по специально заниженной стоимости. В результате последующего обмана жертвы мошенников перечисляют задаток либо всю сумму, не получая результата.

Запомните! Ни в коем случае не стоит перечислять денежные средства, не убедившись в том, что на самом деле существует организация, услугами которой Вы хотите воспользоваться. Проверьте организацию путём мониторинга сети Интернет, почитайте отзывы, попробуйте связаться с представителями и поинтересуйтесь, каким видом деятельности занимается организация и какие услуги предоставляет.

8. Хищении, совершено посредством сети Интернет под предлогом оказания пассажирских услуг через сервис (приложение) по поиску попутчиков «BlaBlaCar»: Данные преступления совершаются в результате размещения объявления через приложение. Для этого лица, как правило, переходят для общения в мессенджер «WhatsApp», где в ходе переписки преступник скидывает ссылку для оплаты либо бронирования поездки, пройдя по которой жертва вносит реквизиты банковской карты.

Необходимо помнить и знать, что самый надёжный способ передвижения – это передвижение на транспорте, по купленным билетам в кассах аэропорта, железнодорожного и автовокзалах. Если же Вы решили воспользоваться сервисом по поиску попутчиков «BlaBlaCar», то необходимо передавать деньги за поездку только из рук в руки при встрече в автомобиле или по прибытию к месту назначения.

9. Хищение, совершено посредством сети Интернет, путём размещения информации о предоставлении услуг досуга. В данной ситуации, до совершения преступления, потерпевший самостоятельно находит предложения в интернет-среде о предоставлении данных услуг. Жертва связывается с злоумышленником по указанным абонентским номерам и под предлогами оплаты услуг, страховки переводит денежные средства на указанные счета посредством мобильного банка или терминала оплаты.

Не стоит пользоваться данными видами услуг, т.к. организация данного вида деятельности запрещена на территории РФ и влечет за собой административную и уголовную ответственность.

10. Хищение совершено посредством сети Интернет под предлогом заработка при «игре» на бирже, инвестирования. Данные преступления совершаются в результате поиска потерпевшими дополнительного источника

дохода. Как правило, потерпевшие оставляют в сети интернет заявку на регистрацию и спустя некоторое время им перезванивает злоумышленник, который предлагает создать личный кабинет на платформе одной из бирж либо перечислить денежные средства для инвестирования, а также убеждает потерпевшего установить программы удалённого доступа «Team - Viewer» или «AnyDesk» с целью оказания «помощи» и контроля за личным кабинетом потерпевшего. После чего жертва под влиянием злоумышленника систематически перечисляет денежные средства различными сумма на лицевой счет, который отображается в личном кабинете биржи либо на банковские карты мошенников, думая, что инвестирует денежные средства. Злоумышленник, в свою очередь, закрывает доступ к личному кабинету, и потерпевший не может вывести данные денежные средства. Для этого его убеждают в необходимости внесения дополнительной суммы денег.

Если Вы все - таки решили заработать данным видом, то следует играть на проверенных биржах, а также пользоваться услугами проверенных лиц (брокеров), занимающихся данной деятельностью. Также следует осознавать риск потери своих денежных средств при игре на бирже, инвестировании, в том числе очень крупных сумм.