Информационно-справочный материал
по профилактике дистанционных хищений

Оперативная обстановка по линии противодействия дистанционным хищениям остается сложной. В регионе по итогам 9 месяцев зарегистрировано 6347 хищений, совершенных дистанционным способом. Раскрыто 661 кража с банковских карт и 358 мошенничеств. Процент расследованных хищений в 2024 году составил 15,9%. У жителей края в 2024 году похищено более 1 миллиарда 606 миллионов рублей. К уголовной ответственности за совершение дистанционных хищений привлечено 859 лиц.

Наибольшую общественную опасность представляют преступления, совершенные с использованием методов социальной инженерии. Этим преступлениям присущи крупные материальные ущербы как собственных накоплений, так и заемных денежных средств. Человек остается без денег и с большими кредитными обязательствами. Такие преступления в структуре дистанционных мошенничеств составляют 60,5%.

Мошенники придумывают новые способы введения в заблуждение, проводят работу над ошибками в случаях, когда потерпевшие не поддались на их уловки.

Наиболее актуальным способом в настоящее время является **звонок потерпевшему на мобильный телефон от представителя сотового оператора с вопросом об окончании договора на обслуживание его абонентского номера.** При необходимости продления срока договора потерпевший называет свои персональные данные для прохождения верификации.

Имеют место **звонки потерпевшим от представителя «Социального фонда» с информацией о некорректном подсчете стажа работы, на основании чего потерпевший получает заниженную пенсию, в связи с чем необходимо явиться в Пенсионный фонд.** «Давайте запишем Вас к сотрудникам. Продиктуйте данные, назовите код из СМС».

По такой же схеме **звонок из медицинских учреждений о необходимости прохождения обследования. «**Давайте я вас запишу, назовите код из СМС».

Одновременно мошенники пытаются переустановить пароль на вход в Госуслуги, о чем потерпевшему приходит СМС, которую он передает мошенникам. Через 30 минут на телефон поступает звонок от человека, представляющегося сотрудником ФСБ, который утверждает, что замечены подозрительные операции по банковским счетам и картам, выясняет, передавали ли кому-либо персональную информацию. После этого, введя потерпевшего в стрессовое состояние, соединяет с сотрудником Центробанка, который должен помочь предотвратить мошенничество. Суть общения сводится к тому, что потерпевший должен обналичить свои накопления и перевести их на «Безопасный (резервный)» счет. Также собеседник склоняет потерпевшего к получению кредитов в максимально возможном количестве банков с целью повышения кредитной нагрузки на себя для того, чтобы мошенники не могли

дистанционно этого сделать. А кредитные денежные суммы внести на безопасные счета банка, по которым не идут проценты.

Следует отметить, что «Безопасных (резервных)» счетов не существует. Это уловки мошенников.

По схожей схеме совершаются преступления:

- Звонок сотрудника банка: «Заявка на переподключение абонентского номера к вашей карте, спорные операции по карте, необходимо обновить «антивирус» или установить программу «Алтайкрайэнерго», скачать программу ТаймВивер, ЭниДеск (программы удаленного доступа к смартфону потерпевшего)».

- Звонок сотрудника правоохранительного органа: «Принять участие в разоблачении сотрудников банка, мошенников. Для этого необходимо оформить кредит и перевести на счет. С Вашей карты осуществлен перевод денег на Украину для финансирования ВСУ. Будет возбуждено уголовное дело. Если это были не вы, необходимо обезопасить себя и на время перевести деньги на счет. Задержан фигурант», – называют его ФИО, «который с нотариальной доверенностью в Москве пытается обналичить Ваши денежные средства».

- Звонок или сообщение, письмо на электронную почту потерпевшего от сотрудника Госуслуг с информацией о взломе и утечке их базы.

- Создание аккаунтов-двойников в мессенджерах от имени руководителей предприятий, учреждений, организаций, государственных органов. Указываются полные данные руководителя, его фотография и т.д. В последующем на телефоны подчиненных сотрудников приходят текстовые сообщения о необходимости содействия кураторам по линии ФСБ, которые сами на него выйдут.

При этом мошенники могут предоставлять вам информацию о месте жительства, счетах, остатках денежных средств, родственниках, автомобилях, заявках о кредитах.

Кроме того, мошенники предоставляют вам фотографии служебных удостоверений, копий договоров на обслуживание «Безопасного» счета, доверенностей.

Также вам на телефон могут приходить заявки об одобрении кредитов в нескольких банках.

Мошенники могут заставить перепроверить через базы принадлежность телефонов к правоохранительным органам, называют руководителей.

Следует отметить, что для гражданского законодательства не важно, кто признан потерпевшим по уголовному делу. Всю материальную ответственность несет заемщик. Он нарушает условия обслуживания банковской карты, предоставляет код, который является электронной подписью кредитного договора.

Как себя обезопасить:

1. Не отвечайте на неизвестные звонки.

2. Установите через оператора связи функцию автоопределения номера.

3. Если Вы клиент ПАО Сбербанк и ВТБ – активируйте через мобильные приложения самозапрет на кредитование или ограничьте его сумму.

4. Установите в мобильном приложении Госуслуг дополнительную защиту данных.

5. Знайте, сотрудники правоохранительных органов никогда не будут заставлять вас производить манипуляции с вашими накоплениями. Помните, сотрудники безопасности банков не будут спрашивать у Вас номер карты, код и ваши данные.

6. Если стали жертвой преступников, сохраните чеки, не удаляйте переписку, сделайте скриншот. Запишите голос мошенника.

7. *Сообщите в полицию.*

Наиболее распространенные способы совершения дистанционных хищений денежных средств.

Инвестирование денежных средств, биржа. Потерпевший, по ссылке в сети-Интернет, проходит на фишинговый сайт[1]. Через некоторое время поступает звонок от менеджера, брокера с предложением перейти в скайп или сторонние мессенджеры. В ходе общения мошенники заманивают большими процентами от вкладов, вносятся малые суммы, дают вывести сумму до 50000 руб. Далее создают иллюзию что вы зарабатываете, видите рост на брокерском счете. Но при попытке вывода денежных средств вас блокируют и больше на связь вы ни с кем не выйдете.

Купля-продажа товаров и услуг на различных электронных площадках Авито, Юла. Не переходите на оплату по ссылкам полученным через сторонние мессенджеры. Не вводите номер карты, код. Вся информация попадает к мошенникам. Выясните, нет ли между продавцом и покупателем посредника, который вводит всех в заблуждение.

«Родственник попал в ДТП». Только в 2024 году зарегистрировано 175 преступлений, задержано 62 пособника-курьера, как правило молодые люди от 15 до 25 лет.

Оказание оккультных услуг, гадание, ворожба. Люди, попавшие в трудную жизненную ситуацию, с целью исправить своё положение обращаются к гадалке (магу, колдуну), переводят денежные средства за услугу. Однако злоумышленник не производит никаких действий, а лишь завладевает деньгами потерпевшего. Как правило указанный вид мошенничества совершают лица цыганской народности.

Получение компенсации за бады. В последнее время распространена схема написания заявления на министра юстиции Чуйченко И.Ф. с просьбой выделения адвоката для представления интересов при расследовании уголовного дела. Через некоторое время выходит на связь адвокат и требует для вступления в дело сумму от 25000 до 70000 руб. Никто и никогда в крае не получал компенсацию.

[1] Сайт злоумышленников, который выглядит идентично другому (настоящему) сайту (пример: wkontakte.ru вместо vkontakte.ru)

Оказание интим услуг, предоплата. Потерпевший, желая воспользоваться интим услугами, связывается со злоумышленником, который берет предоплату. В последующем на связь не выходит, интим услугу не предоставляет.

Вымогательство денежных средств за нераспространение сведений интимного характера в сети Интернет. В основном страдают молодые люди, пересылая интимные фотографии.

Взлом страниц, требование о переводе денежных средств. Потерпевшему поступает звонок или сообщение о взломе страницы в социальной сети. Потерпевшие, с целью её разблокировки, переводят деньги на карты, фотографии которых пересылают мошенники.

В последнее время изменяется способ криминальных транзакций. Если банки начали блокировать переводы с карты на карту, то в настоящее время потерпевших принуждают скачать приложение Mir Pay, привязать карту подконтрольную мошенникам. После перевода денежных средств на карту злоумышленники просят удалить приложение. Такие операции банками не блокируются, а в чеках с банкоматов видны маски счетов, куда перечисленны денежные средства. Установление счета по маске занимает продолжительное время.

Также вызывает озабоченность вовлечение молодежи в процесс обналичивания денежных средств. Молодые люди оформляют на себя банковские карты и за денежное вознаграждение передают их третьим лицам. Следует предупредить таких лиц, что у потерпевших есть возможность взыскать денежные средства, которые поступили на Вашу карту в рамках гражданского законодательства ст. 1002 Гражданского Кодекса Российской Федерации «Неосновательное обогащение». Такая практика в крае имеется, 10 потерпевших по инициативе органов внутренних дел получили положительные судебные решения, в свою очередь адвокатская палата помогла бесплатно в сопровождении исковых заявлений.

Если есть карты, которые переданы третьим лицам, необходимо срочно обратиться в банк закрыть их. Иначе будьте готовы, что кто-то из потерпевших в течении исковой давности, которая составляет 3 года, может взыскать с вас денежные средства.

В настоящее время каждому из потерпевших разъясняется возможность обращения в гражданский суд о взыскании неосновательного обогащения.

Кроме того, в крае наработана правоприменительная практика привлечения номинальных владельцев банковских карт за их продажу третьим лицам к уголовной ответственности. Только в 2024 году возбуждено по ст. 187 УК РФ «Неправомерный оборот средств платежей» 216 уголовных дел, 147 дел направлены в суды для рассмотрения по существу.

ГУ МВД России по Алтайскому краю