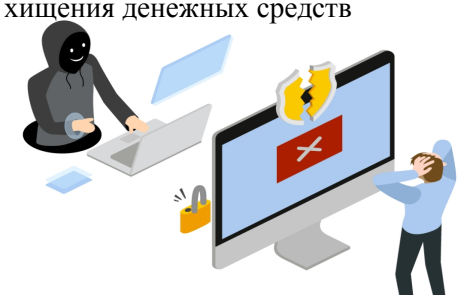
На территории Оренбургской области правоохранительными органами все чаще регистрируются факты совершения хищений денежных средств с лицевых счетов граждан с использованием современных информационно-телекоммуникационных технологий. Потерпевшими становятся жители региона различных возрастных групп. Преступники при совершении хищений постоянно совершенствуются, придумывая новые способы, при этом активно используют Интернет-ресурсы, торговые площадки, возможности цифровой телефонии.

Популярным способом хищения денежных средств в сфере ИТТ является **завладение конфиденциальной информацией**, предоставляющей доступ к персональным данным владельца, в ситуации передачи самим владельцем таких данных, находясь под влиянием злоумышленника.

Так, зачастую преступники используют арендованные (как правило виртуальные) мобильные номера, которые не оформляются на конкретное физическое лицо, в связи с чем достаточно сложно установить не только конкретное устройство, а и определенный регион из которого осуществлялся вызов.

Посредством арендованных номеров, преступники могут осуществлять телефонные звонки на абонентские номера граждан, представляясь сотрудниками ФГИС «Единый портал государственных и муниципальных услуг», коммерческих банков, после чего предлагают продиктовать смс-код (являющийся простой электронной подписью, подтверждением списания денежных средств/проведение финансовой операции), направленный на абонентский номер с целью хищения денежных средств



Как не стать потерпевшим от действий злоумышленников в сфере ИТТ?

Безопасность в анализируемой сфере в первую очередь зависит от осведомленности граждан о базовых мерах предосторожности в сфере ИТТ.

Не переходите по подозрительным ссылкам, предлагающим какие-либо выгоды или вознаграждения.

Контролируйте операции по вашей банковской карте, так как в случае неправомерного доступа и попытки хищения денежных средств, необходимо обратиться в службу поддержки Вашего банка для заморозки и операций по карте.

Используйте усложненные пароли, которые будут содержать буквенный и цифровой набор (не используйте даты рождений, повторяющиеся числа).

Помните, что в случае поступления предложений предоставить данные банковской карты, установить какое-либо приложение либо указать иную информацию, к ним стоит относиться критически, информацию перепроверять путем самостоятельных звонков на горячую линию, службы поддержки.

При поступлении звонков либо получения сообщений от «родственников» прежде, чем переводить денежные средства необходимо самостоятельно созвониться с ними, выяснить их местонахождение и иные обстоятельства. При утрате банковской карты необходимо незамедлительно обращаться по горячей линии банка и требовать заблокировать утраченную карту.

Преступления в сфере информационно-телекоммуникационных технологий квалифицируются по ст. 159 Уголовного кодекса РФ, то есть мошенничество.

ПОЛИЦИЯ – 102

Отд МВД России по Курманаевскому району

Дежурная часть: 8(35341)2-15-98

8(999)259-39-73

ПРОКУРАТУРА
Российской Федерации

ПРОКУРАТУРА
ОРЕНБУРГСКОЙ ОБЛАСТИ

ПРОКУРАТУРА
КУРМАНАЕВСКОГО РАЙОНА

Профилактика преступлений в сфере информационно-телекоммуникационных технологий

Другим видом обмана являются предложения о вложении в новые виды криптовалют, без заключения каких-либо договоров, когда от потерпевшего требуется лишь перевести деньги либо настоящую криптовалюту на счет мошенников в обмен на обещание удвоить вложения.

Следует отметить, что всё чаще в преступных схемах стали использоваться поддельные (так называемые «фишинговые», «сайт-двойник» или «сайт-зеркало») сайты , имитирующие реальные Интернет-магазины или маркетинговые ресурсы, а в некоторых случаях и сайт банка. При этом различаться такие сайты от настоящих могут в одну букву или цифру. Поддельные сайты создаются с целью сбора у граждан персональных данных и реквизитов их банковских карт.

Появились рассылки и сайты с предложением купить технику, предметы роскоши и другие товары по низким ценам, подключиться к Системе быстрых платежей, льготному обмену валют по выгодному курсу.

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.

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, 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

Мошенничество в социальных сетях

Хищение совершено с использованием сети Интернет в социальных сетях («Одноклассники», «ВКонтакте»,), 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.

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.

Хищения также совершают 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».

Ни при каких условиях нельзя переходить по сомнительным Интернет-ссылкам, сообщать третьим лицам остаток денег на счетах, банковских картах, их номера, сроки действия, CVC/CVV-коды с оборота карт и коды из СМС-сообщений, приходящих с сервисных телефонных номеров банков.

Рекомендуется пользоваться и вводить платежную информацию только на проверенных сайтах, а при поступлении сомнительных звонков либо сообщений-прекращать диалог.

В случае поступления звонков, подозрительных сообщений или совершении иных мошеннических действий необходимо обратиться в правоохранительные органы.