Способы хищений денежных средств, совершенных с использованием информационно-телекоммуникационных технологий

Способы совершения IT-преступлений (первый контакт с потерпевшим):

- номера IP-телефонии, абонентские номера;
- ссылки на различные Интернет-сайты;
- сайты объявлений (например, «Авито», «Юла»);
- социальные сети;
- установка программ удаленного доступа;
- рассылка сообщений на электронные почтовые адреса
- оплата товаров и услуг с утерянной банковской карты, переводы «Банк онлайн», снятие денежных средств.

Исходя из этого, некоторые **технические способы списания** денежных средств:

- назвать номер банковской карты, CVC-код (3х-значный номер на оборотной стороне карты). В данном случае у злоумышленников появляется возможность приобретения товаров и услуг в сети Интернет. Пароль при оплате запрашивается в зависимости от выбранного лимита Интернет ресурса, то есть, если лимит установлен 10 000 рублей, то пароль будет запрошен при покупке свыше 10 000 рублей;
- назвать все реквизиты карты, в том числе пароль, пришедший в смс сообщении. Появляется все возможности для управления финансами на банковской карте;
- скачать программу удаленного доступа (AnyDesk, TeamViewer, QuickSupport и другие). В случае, если назвать 6-ти значный номер рабочего стола, который прописывается в самой программе, то все процессы возможно проводить удаленно. С целью обезопасить себя, не устанавливать любые программы по просьбе третьих лиц, особенно, если нет необходимых знаний для целевого использования и его функционала;
- Фишинг. Распространение ссылок, писем на электронную почту. Под различными предлогами злоумышленники отправляют ссылку на сайт, в котором имеется возможность ввода реквизитов банковский карт. После ввода данной информации, денежные средства поступают на подконтрольные мошенникам счета, финансовые кошельки. Кроме того, могут быть взломанные сайты, создаются Интернет-сайты «двойники», сайты-опросники для сбора необходимой информации для злоумышленников.

Наиболее распространенные способы IT-мошенничеств:

1. Покупка товаров/услуг на сайте «Авито». (продажа породистых щенков, покупка различных вещей,

Потерпевший находит объявление. При переписке с мошенником, обговариваются условия, при которых потерпевший указывает

злоумышленнику, что готов приобрести товар/услугу только при помощи «Авито доставка». Злоумышленник соглашается, при этом скидывает потерпевшему ссылку, якобы «Авито доставка» (причину отправки данной ссылки от «Авито» ему, а не потерпевшему не известна). Пройдя по ссылке, потерпевший вводит в соответствующие графы все реквизиты своей банковской карты и пароли в смс. После чего, у потерпевшего списываются денежные средства в размере стоимости товара/услуги. Однако, злоумышленник указывает, что денежные средства не поступили и мошеннику снова присылают ссылку якобы служба поддержки «Авито», скидывает потерпевшему. Потерпевший в ходе общения со «службой поддержки Авито» узнает, что денежные средства не списались, но для возврата денежных средств необходимо пройти по новой ссылке, где снова нужно ввести все реквизиты карты для возврата денежных средств. После выполнения указанных действий производится новое списание денежных средств. Злоумышленники при попытке повторного обмана, могут указать потерпевшему, что для возврата денег, баланс карты должен соответствовать или быть больше первоначальной транзакции.

В данном случае, для предотвращения несанкционированного списания денежных средств, использовать ссылки, отправленные от покупателя не стоит. Кроме того, для возврата денежных средств баланс карты может и не соответствовать произведенным ранее транзакциям.

2. **Бонусы (розыгрыши) от различных известных банков, реклама от которых размещается в социальных сетях.**

Потерпевший, используя социальные сети, находит красочное объявление о проводимых акций конкретного известного банка (знаменательная дата банка, выигрыш в банковские лотереи, день пожилого человека, пенсионера и прочее), бонусы от которого возможно получить в виде денежных средств. Пройдя по ссылке, появляется простой опросник, по завершению которого для получения денежных средств требуется ввести свои реквизиты банковской карты и пароли в смс сообщении. По результатам выполнения указанных действий, денежные средства мошенники похищают.

Подобных акций банки не проводят, к тому же, не занимаются распространением такого вида реклам.

3. Предложение дополнительного заработка путем участия в ставках на спорт.

В социальных сетях потерпевшему с любого аккаунта (друга, страницу которого взломали, ранее неизвестного человека) поступает сообщение с предложением заработать на ставках на спорт, результаты которых заранее известны представителям злоумышленников. При этом, в ходе переписки мошенники могут скидывать скриншоты переписки с иными лицами, которые якобы уже в таких ставках участвуют и получают денежные средства. Скидывают ссылку на сайт, где необходима регистрация. Потерпевший

регистрируется, после чего, появляются сведения о балансе. Далее, потерпевший по указанию злоумышленников переводит денежные средства на различные банковские карты (счета), финансовые кошельки под предлогом пополнения баланса, оплаты комиссий за предыдущие оплаты и прочее. Никаких выигрышей потерпевший не получает.

Такого рода дополнительного заработка не существует. Достоверно заранее знать истинный результат игры в спорт невозможно.

4. Способ «Незаконная транзакция»

Позвонил мошенник женщине возрастом 40 лет, жительнице г. Ижевска, которая трудоустроена на заводе, представился сотрудником Сбербанка. Злоумышленник указал ей, что по ее счетам происходят незаконные списания на сумму 3 000 рублей в г. Ростов. При этом, в ходе разговора мошенники для входа в более доверительное отношение, общались в теплом разговорном тоне, для придания правдоподобности этой ситуации, переводили на еще нескольких «сотрудников Сбербанка».

Для достоверности гражданам необходимо прервать разговор и перезвонить на контактный номер телефона банка. Номер телефона указан на оборотной стороне банковской карты.

После чего, злоумышленники для предотвращения вышеуказанных действий потребовали назвать номер банковской карты женщины, CVC-код (3х-значный номер на оборотной стороне карты). Данные она назвала.

Имея CVC-код у злоумышленников появляется возможность приобретения товаров и услуг в сети Интернет. Пароль при оплате запрашивается в зависимости от заданного лимита Интернет-ресурсом, то есть если лимит на Интернет-сайте установлен 10 000 рублей, то оплачивать без подтверждения пароля можно до 10 000 рублей.

Далее злоумышленник просит назвать пароль, который пришел в смс сообщении, что она и сделала.

Банковский сотрудник никогда не будет спрашивать эти сведения. Помимо этого, в самом сообщении с паролем, банк прописывает о том, что сообщать данный пароль никому нельзя, даже самому сотруднику банка. В случае если назвать данный пароль, то появляется все возможности для распоряжениями финансами на банковской карте (покупки, переводы на любые счета (карты)).

После того, как потерпевшая указала все реквизиты банковской карты злоумышленникам, у нее произошло списание на 120 000 рублей на различные счета, Киви-кошельки, абонентские номера сотовых операторов, подконтрольные злоумышленникам.

Мошенники могут указать иные предлоги, которые могут послужить предметом последующего разговора (кто-то оформил кредит на потерпевшего, либо потерпевший оставлял Интернет-заявку на кредит, получения различных выигрышей и прочее). Однако, результатом разговора будет лишь получить вышеуказанные реквизиты банковской карты гражданина для того, чтобы похитить денежные средства.

Поэтому, для того, чтобы обезопасить свои денежные средства, сбережения в целях профилактики, необходимо прекратить телефонный разговор, перезвонить на реальный телефон банка, который имеется на оборотной стороне банковской карты, официальном Интернет-сайте, и убедиться в правильности сложившейся ситуации.

Также, злоумышленниками могут быть предложены скачать и установить на сотовый телефон программу для того, чтобы обезопасить свои денежные средства, находящиеся на счетах. Для этого, в ходе общения просят назвать код, который прописывается при входе в данную программу.

Установленные программы являются программами удаленного доступа (AnyDesk, TeamViewer, QuickSupport и другие). В случае, если назвать 6-ти значный номер рабочего стола, который прописывается в самой программе, то все процессы возможно проводить удаленно. С целью обезопасить себя, не устанавливать любые программы по просьбе третьих лиц, особенно, если нет необходимых знаний для целевого использования и его функционала.

В результате выполнения указанных действий всех со счетов производится списание денежных средств.

5. использование социальных сетей (например, «Вконтакте», «Одноклассники»).

Наиболее распространенные схемы в социальных сетях, просьба в долг от «знакомых», приобретение товаров и услуг в соответствующих сообществах, где после оплаты аванса, товар и услуга не направляется потерпевшему.

6. использование на торговых площадках фишинговых страниц, имитирующих популярные платежные сервисы.

Фишинговый сайт – копия популярного сайта, созданная для введения в заблуждение их пользователей (сайты авиакомпаний (для приобретений авиабилетов), торговые площадки (например, «М-Видео» для приобретения компьютерной техники), сайты государственных и муниципальных структур (например, заказ услуги через портал «Госуслуги»). Цель – завладение конфиденциальной информации (логины и пароли регистрации на сайтах, данные банковской карты, номеров телефонов и иной другой информации).

7. обман на сайтах знакомств.

В ходе переписки с потерпевшим, после его психологической обработки, злоумышленники просят перевести на их подконтрольные счета денежные средства под различными предлогами, либо выманивают все реквизиты банковской карты.