Главе муниципального района «Магарамкентский район»

Ахмедову Ф.З.

**ИНФОРМАЦИЯ**

для размещения на официальном сайте администрации района в разделе «Прокуратура разъясняет»

**Противодействие преступности в сфере**

**использования информационно-коммуникационных технологий**

В последнее десятилетие в Российской Федерации хищения с использованием средств связи набирают стремительные обороты. Законодатель, пытаясь сдержать рост указанного вида хищений, реагирует на данную ситуацию. Это подтверждается теми изменениями, которые вносятся в уголовное законодательство. Так, Федеральным законом от 23 апреля 2018 года часть 3 статьи 158 и часть 3 статьи 159.3 УК РФ были дополнены особо квалифицирующим признаком: «деяния, совершенные с банковского счета, а равно в отношении электронных денежных средств». Кроме того, ужесточена санкция за мошенничество с использованием электронных средств платежа: арест на срок до четырех месяцев заменен на лишение свободы на срок до трех лет.

Подчеркивая общественную опасность преступлений, предусмотренных за мошенничество с использованием электронных средств платежа и в сфере компьютерной информации, законодатель снизил пороговое значение крупного размера с одного миллиона пятисот тысяч рублей до двухсот пятидесяти тысяч рублей, особо крупного – с шести миллионов рублей до одного миллиона рублей.

Все рассматриваемые хищения денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, можно разделить на две основные группы:

1) бесконтактные, то есть совершаемые без личностного контакта субъекта с потенциальным потерпевшим (преступления, в которых субъект не контактирует с потерпевшим);

2) контактные, то есть совершаемые посредством установления личностного контакта субъекта с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения).

Подавляющее большинство анализируемых хищений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании психологических слабостей человека и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Так называемый фишинг - тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо как правило содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия используется также для распространения троянских коней: эксплуатируется любопытство, либо алчность объекта атаки. Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперсылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

Кроме того, мошенники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Цель злоумышленников — получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. Просим принять во внимание, что сотрудник банка не имеет право спрашивать пароль от карты и уж тем более, его нельзя никому сообщать. Чтобы не стать жертвой подобной аферы, достаточно позвонить в банковскую организацию по телефону, указанному на официальном сайте или на обороте карты. Уточните у оператора, действительно ли кто-то пытается снять деньги, и сообщите номер телефона мошенников.

Помощник прокурора района

юрист 2 класса К.М. Раджабов