**Прокуратура разъясняет: Мошенничество в сфере IT-технологий.**

Тенденция развития информационных технологий в последнее время влечет повсеместное их вовлечение во многие сферы общественных отношений, что сказывается не только на удобстве для добросовестных пользователей, но и служит почвой для противоправной деятельности, выражающейся в незаконном обогащении, дискретизации граждан и государственных органов, распространении запрещенной информации, в том числе, идей экстремизма и терроризма.

Как в целом по стране, так и на территории Томской области отмечается ежегодный рост таких преступлений, к которым также относятся хищения денежных средств с банковских счетов физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Большинство рассматриваемых преступлений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей (сотовой связи, ресурсов сети «Интернет»). Данная преступная технология основана на использовании слабостей человеческого фактора и является достаточно эффективной.

К примеру, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выяснить [**конфиденциальные**](https://ustdoneckiy.bezformata.com/word/konfidentcialnoj/18227/) данные банковской карты, сославшись на необходимость решения проблемы при работе в компьютерной системе или с банковским счетом, дезинформируя о его блокировке либо попытке совершения противоправных действий со стороны третьих лиц.

Также преступники зачастую представляются близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. Например, в связи с необходимостью освобождения их от уголовной ответственности, разрешению в пользу близкого человека, якобы, виновного в ДТП, при этом нередко такие лица сами выдают себя за сотрудников правоохранительных органов.

Так же имеют место и так называемые дистанционные формы хищения денежных средств,  совершаемые путем размещения на сайтах по продажам в сети «Интернет» заведомо ложных предложений о продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица без фактической передачи приобретаемого товара либо предоставлении несоизмеримых по стоимости предметов.

Кроме того, нередко денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них [банковскими](https://ustdoneckiy.bezformata.com/word/bankovskom/1853/) сервисами или банковские карты: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – денежные средства снимаются в банкоматах.

Так же, в последнее время распространение получил, так называемый, «фишинг» - один из методов «социальной инженерии», направленный на получение конфиденциальной информации, при котором 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](https://ustdoneckiy.bezformata.com/word/sotcialnaya-inzheneriya/4611690/)» 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 гиперссылкам. 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.

За совершение таких деяний, в зависимости от способа совершения преступлений, предусмотрена уголовная ответственность по ст. 158, 159 УК РФ.

В случае, если Вы стали жертвой вышеуказанных мошенников, обращайтесь в ближайший отдел полиции.

 Помощник прокурора района

юрист 3 класса Болдакова О.С.