ПРОКУРАТУРА КАМЕНСКОГО РАЙОНА ПРЕДУПРЕЖДАЕТО МОШЕННИЧЕСТВЕ В СФЕРЕ IT-ТЕХНОЛОГИЙ

На протяжении последних лет на территории Каменского района и Свердловской области в целом наблюдается рост хищений, совершенных с использованием информационно-телекоммуникационных технологий. Основной причиной данных преступлений является низкая «цифровая» и финансовая грамотность.

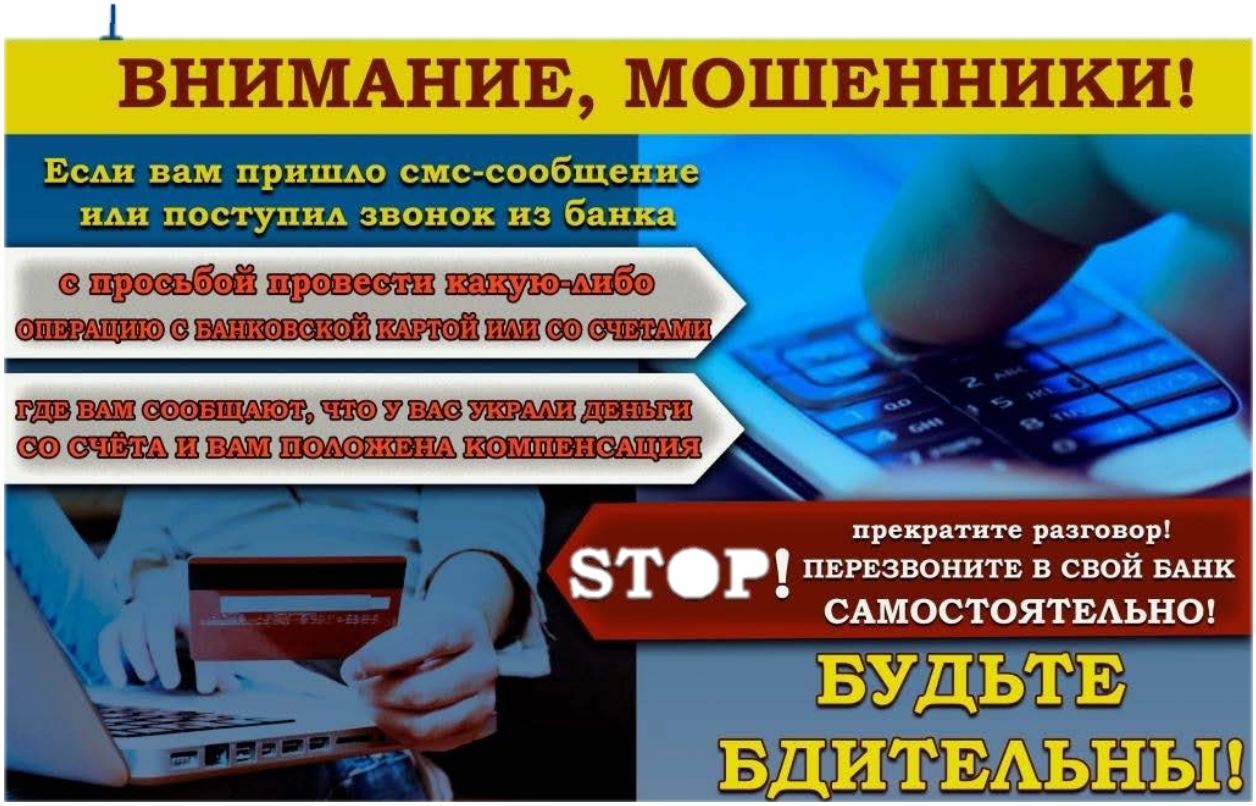
Способы совершения данных преступлений разнообразны. Распространенный характер носят случаи телефонных звонков мошенников под видом представителей банков, которые под разными предлогами пытаются получить от граждан реквизиты банковских карт, с помощью которых впоследствии переводят денежные средства на свои счета, либо побуждают граждан самостоятельно осуществить такие переводы. Основным аргументом мошенников является ложная информация о попытке хищения и необходимости перевода денежных средств на «безопасный» счет, который является счетом мошенников.

Другим распространенным способом является публикация мошенниками объявлений в сети Интернет о продаже товаров и об оказании услуг. После перевода потерпевшим денежных средств злоумышленнику товар не поставляется и услуги не оказываются, а злоумышленник перестает отвечать на сообщения и телефонные звонки.

Увеличивается число случаев так называемого «фишинга». Это вид интернет-мошенничества, целью которого также является побуждение потерпевшего поделиться своей конфиденциальной информацией, в том числе паролем, логином или номером банковской карты. Создатели фишинговых сайтов проводят массовые рассылки электронных писем, личных сообщений внутри различных сервисов, например от имени банков, со ссылкой на сайт, внешне схожий с настоящим. После перехода по ссылки мошенники пытаются любыми способами побудить пользователей ввести личные данные, таким образом получая доступ к аккаунту и банковским счетам.Чтобы избежать утечки данных необходимо предварительно проверить сайт на признаки фишинга. Например, он может содержать неправильное доменное имя. В основном мошенники регистрируют схожие домены, которые отличаются только одной буквой или символом. Кроме того, необходимо обратить внимание и на дизайн сайта, который может быть устаревшим, а также на наличие орфографических ошибок. Всё это может свидетельствовать о том, что Вы на фишинговой странице.

Прокуратура Каменского района призывает граждан быть бдительными, не сообщать никому данные банковской карты, счета и код безопасности, не использовать сомнительные ссылки на фиктивные сайты банков, интернет-магазинов и не вводить на них свои персональные данные аутентификации. Не переводить денежные средства, даже если лица представляются сотрудниками кредитных организаций или правоохранительных органов.Если Вам известны сайты, используемые для хищения денежных средств, сообщите о них в правоохранительные органы.

Прокуратура предупреждает: только Ваша бдительность поможет предотвратить преступление, и, если оно все же произошло, обратитесь в полицию. Будьте внимательны и не позволяйте злоумышленникам Вас обмануть.



ПРОКУРАТУРА КАМЕНСКОГО РАЙОНА ПРЕДУПРЕЖДАЕТО МОШЕННИЧЕСТВЕ В СФЕРЕ IT-ТЕХНОЛОГИЙ

К типичным вариантам мошенничества с банковскими картами он-лайн следует отнести, например:

1. При продаже товара или покупке с рук мошенники – потенциальные покупатели или продавцы – просят не только номер карты, но и секретные данные. Этого делать ни в коем случае нельзя!
2. Ваш друг в социальных сетях просит одолжить деньги или отправляет Вам странную ссылку. В таком случае свяжитесь с другом и уточните, действительно ли ему нужна помощь, а также узнайте о достоверности той информации, которую он направил.
3. На Вашу электронную почту приходит письмо с информацией о выигрыше или с предложением работы, которую Вы не искали. В таком случае используйте спам-фильтры, чтобы не попасться на подобную уловку мошенников, а также внимательно изучайте то, что приходит на Вашу почту с незнакомых электронных адресов.
4. Вы перешли на известный сайт, например, ГИБДД или ФНС, однако, заметили некие изменения, которые не замечали ранее – лишняя буква в строке браузера, измененный номер телефона для связи с той или иной службой. Поэтому, при переходе на тот или иной сайт/портал внимательно изучайте его содержание, а также добавьте в закладки браузера те сайты, которыми Вы часто пользуетесь.

Помните о том, что нельзя сообщать посторонним лицам CVV или CVC-коды, ПИН-код банковской карты, срок действия, пароли из банковских уведомлений.

Будьте внимательны и осторожны!

В случае совершения в отношении Вас мошеннических действий сразу же сообщите об этом в правоохранительные органы.

Подробнее о том, как можно защитить себя от киберкраж и финансовых мошенниках читайте на сайте fincult.info.

ПРОКУРАТУРА КАМЕНСКОГО РАЙОНА ПРЕДУПРЕЖДАЕТ ОМОШЕННИЧЕСТВЕ 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, дискредитации граждан и государственных органов, распространении запрещенной информации, в том числе, идей экстремизма и терроризма.

Как в целом по стране, так и на территории Свердловской 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 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.

Также имеют место и так называемые дистанционные формы хищения, 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 сервисами или банковские карты: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа - деньги снимаются в банкоматах.

Кроме того, 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 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.ст. 158, 159, 159.3, 159.6 УК РФ.

В случае, если Вы стали жертвой указанных выше мошенников необходимо обратиться в ближайший отдел полиции.

Изменить эту ситуацию возможно в том случае, если граждане при общении с неизвестными лицами будут проявлять повышенную бдительность и более ответственнее подходить к сохранности своих сбережений.