

Учредитель администрация муниципального образования Ивановского сельсовета Баганского района Новосибирской области

15.07.2020

«Бюллетень **органов местного самоуправления муниципального образования Ивановского сельсовета**.»

№9(228)

**ПРОКУРОР РАЗЪЯСНЯЕТ**

**Хищения, совершаемые с использованием современных информационно-телекоммуникационных технологий**

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи информационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение запрещенной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» введена ответственность виновных лиц по статье 158 УК РФ за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ).

Аналогичным образом, с целью усиления уголовной ответственности за противоправные действия с использованием электронных средств платежа, изменены диспозиции и санкции статей 159.3 и 159.6 УК РФ.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые на практике нередко используются в качестве инструментария завладения чужим имуществом.

В целях борьбы с компьютерной преступностью уголовным законом предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).

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 слабостей человеческого фактора 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.

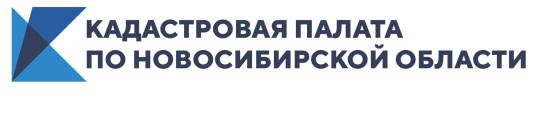
Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

Заместитель прокурора района

О.Г. Тимошенко

****

**Новосибирцы могут получить выписку из ЕГРН в бумажном виде**

**не выходя из дома**

*У новосибирцев появилась возможность заказать и получить выписку сведений из Единого государственного реестра недвижимости (ЕГРН) не выходя из дома и без использования электронной подписи при получении сведений ограниченного доступа, работая с электронными сервисами*

Дистанционное решение вопросов оформления недвижимости имеет массу преимуществ, так как экономит временные и финансовые затраты. Данный способ получения госуслуг сейчас особенно актуален – в условиях современной эпидемиологической обстановки, когда рекомендуется не посещать общественные места.

В июле этого года [Кадастровая палата по Новосибирской области](https://vk.com/kadastr_nso) начала оказаниенового вида услуг для граждан. Теперь заявители могут заказать выездной прием запросов о предоставлении сведений ЕГРН, а также курьерскую доставку готовых документов без посещения офисов [МФЦ](https://www.mfc-nso.ru) и использования специальных электронных сервисов.

Специалисты выезжают на дом, в офис или любое удобное для заявителя место в заранее согласованное время. Кроме того, оборудование, необходимое для приема-выдачи документов, специалист привезет с собой.

Получение услуг доступно на всей территории г. Новосибирска, кроме Советского и Первомайского районов, а также микрорайона Пашино Калининского района. Стоимость услуг по выездному приему запросов и курьерской доставке документов для физического лица составляет 1000 рублей; для юридического лица – 1500 рублей. На безвозмездной основе услуга оказывается ветеранам и инвалидам Великой Отечественной войны, инвалидам I и II групп (указанные лица должны быть правообладателями объектов недвижимости).

Оставить заявку на получение услуг можно любым удобным способом:

- по телефону: 8 (383) 349-95-69 (доб. 2146), факс (8383) 346-16-17;

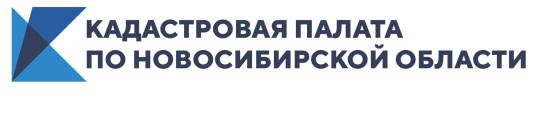
- с помощью ВЦТО: 8 (800) 100-34-34;

- по электронной почте [vpd@54.kadastr.ru](mailto:vpd@54.kadastr.ru);

- почтовым отправлением: 630087, г. Новосибирск, ул. Немировича-Данченко, д. 167, оф. 703, филиал Кадастровой палаты по Новосибирской области;

- лично: г. Новосибирск, ул. Немировича-Данченко, д.167, каб. 322/1.

Напомним, с 2017 года выписка из ЕГРН является единственным документом, подтверждающим право собственности на объект и предоставляющим из реестра недвижимости достоверную и актуальную информацию о недвижимости. Свидетельства о госрегистрации прав, выдаваемые гражданам ранее, сохраняют свой статус и имеют такую же юридическую силу. Выписка используется для подтверждения права собственности при проведении сделок, определения налоговых обязательств собственников, при открытии наследства, оспаривании сделок в суде, подготовке процедуры дарения и т.д.

****

**О внесении в ЕГРН сведений о границах населенных пунктов расскажут в Кадастровой палате**

*В среду, 29 июля, пройдет очередная горячая линия Кадастровой палаты по Новосибирской области*

В Новосибирской области насчитывается более 55% населенных пунктов, сведения о границах которых содержатся в ЕГРН. О порядке внесения в ЕГРН таких сведений расскажут эксперты региональной Кадастровой палаты в рамках горячей линии.

Звонки будут приниматься с 10.00 до 12.00 по телефону: 8 (383) 349-95-69. На вопросы граждан ответят начальник отдела инфраструктуры пространственных данных Олеся Кучерова (доб. 2902) и заместитель начальника отдела Вероника Сухорукова (доб. 2901).

Редактор

А.К.Ритер

Тираж 4.

объем 3 п.л.

Бесплатно

Адрес редакции: 632787

С. Ивановка, ул. Центральная,27

Телефон 39-219

|  |
| --- |
|  |