

МВД России ГЛАВНОЕ УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ по г. САНКТ-ПЕТЕРБУРГУ и ЛЕНИНГРАДСКОЙ ОБЛАСТИ ГУ МВД России по г. Санкт-Петербургу и

ЛЕНИНІ РАДСКОЙ ОБЛАСТИ (ГУ МВД России по г. Санкт-Петербургу и Ленинградской области)

	Partition Comments,	
Лиговский пр., о.1	45. Санкт-Петербуј	рг, 191119
	Nº	
Ha №	от	

Председателю Комитета по вопросам законности, правопорядка и безопасности Санкт – Петербурга

О.И. Аришиной

Уважаемая Ольга Ивановна!

Анализ состояния законности в Санкт-Петербурге показал, что структура преступности претерпела серьезные изменения. При снижении регистрации уличной преступности в целом злоумышленник стали значительно чаще совершать преступления в сфере информационно-телекоммуникационных технологий, связанных с хищениями денежных средств граждан с использованием сети «Интернет» и средств мобильной связи – так называемые бесконтактные или дистанционные способы хищений.

Удельный вес таких преступлений составил 22,2 %, что, безусловно, вызывает необходимость кардинального изменения подхода к борьбе с ними. В настоящее время каждое седьмое преступление в стране совершается в указанной сфере. Причем наибольшие темпы прироста имеют преступления, связанные с использованием или применением расчетных пластиковых карт и средств мобильной связи. При этом в условиях стремительного развития современных технологий способы совершения таких преступлений становятся все более разнообразными и изощренными

Учитывая стремительный рост преступлений, совершенных в указанной сферс, Министерством внутренних дел Российской Федерации и ГУ МВД России по г. Санкт-Петербургу и Ленинградской области расследование уголовных дел данной категории поставлено на особый контроль.

Как правило, жертвами мошенников при совершении хищений в данной сфере становятся наиболее незащищенные слои населения (лица преклонного возраста, пенсионеры, подростки), а так же лица, не обладающие навыками пользования компьютерными и мобильными техническими устройствами.

Наиболее распространенными являются следующие способы хищений:

1) Мошенничества с банковскими картами, при совершении которых потерпевшему на мобильный телефон поступает звонок якобы от службы безопасности банка и сообщается ложная информация об ошибочном переводе

денежных средств, которые преступники требуют вернуть путем их перевода на сообщаемый ими потерпевшему счет, или «угрозе» блокировки банковской карты якобы по причине сбоя в программном обеспечении кредитной организации (Банка) либо попытках несанкционированного списания денежных средств со счета потерпевшего с дальнейшим развитием событий по вышеуказанному сценарию. К данному разделу относится и «Приобретение сети Интернет», услуг посредством когда используются замаскированные сайты-двойники, посредством злоумышленник получает данные банковской карты потерпевшего, доступ к его счету, с которого списываются денежные средства. Главная цель мошенников – получение у потерпевшего номера пин-кода и номеров CVVколов.

- 2) «Случай с родственником». В телефонном разговоре мошенники сообщают потерпевшему о необходимости оказания помощи его близкому человеку или родственнику, который якобы попал в беду, к примеру, в связи с совершением им преступления, просят оказать финансовую помощь.
- 3) Телефонные мошенничества, в ходе которых потерпевшему сообщается об участии в розыгрыше призов (участие в лотерее, получение компенсация за работу в советское время, за ранее приобретенные некачественные биоактивные добавки, пандемию), предлагается перевести денежные средства за пересылку товара, оплатить пошлины, проценты и т.п., либо просят указать счет, номер карты, куда якобы будет осуществляться перевод. Также мошенники могут представиться сотрудниками социальных служб, сообщить о возможности приобретения льготных путевок, выгодного обмена денежных средств и т.п.
- 4) Телефонный вирус. На телефон (на электронную почту) абонента приходит сообщение с просьбой перейти по определенной ссылке, либо предложение установить программу (являющуюся вредоносной) под предлогом защиты от посягательств на денежные средств и пр. При переходе по ссылке (установке программы) на телефон скачивается «вирус» и происходит списание денежных средств со счета.
- 5) Злоумышленники взламывают персональную страницу пользователя в социальных сетях или мессенджере и отправляют сообщения с просьбой перевести деньги в долг от имени друга, либо появляется информация о необходимости собрать деньги на лекарства для спасения чьей-то жизни.

Приведенный перечень способов хищений не исчерпывающий, есть еще «брачные мошенничества», сообщения о несуществующем наследстве, участие в брокерских сделках и т.д. Но по смыслу каждой из вышеуказанных схем хищений основной задачей злоумышленников является установление доверительного контакта с потерпевшим, в том числе используются так называемые методы социальной инженерии (психологических знаний, умений,

приемов), а потом уже создание условий, при которых денежные средства потерпевшего незаконным путем переходят в распоряжение преступников.

Принимая во внимание, что рассматриваемая категория преступлений имеет наибольшую общественную опасность, так как обусловлена высокой степенью латентности и неуязвимости, и направлена на отъем личных средств наименее защищенных слоев населения, отличающихся недостаточной грамотностью в финансовой и информационно-телекомуникационной сферах, требуется на всех уровнях законодательной и исполнительной власти максимально сосредоточить усилия для эффективной борьбы с преступностью, активно использующей компьютерный прогресс и IT-технологии.

С учетом изложенного, и в целях укрепления правопорядка в Санкт-Петербурге, предлагаю реализовать в пределах полномочий комплекс активных мер профилактики преступлений в данной сфере, в первую очередь, направленный на информирование населения Санкт-Петербурга существующих способах мошенничеств разъяснение необходимых И превентивных правил поведения, а также повышение уровня необходимых знаний в финансовой и информационно-телекомуникационной сферах путем проведения соответствующих лекций, семинаров; реализации различных социальной рекламы (устное информирование, размещение социальных плакатов, баннеров, листовок, социальных роликов, брошюр, стендов и т.д.).

О результатах рассмотрения настоящего письма и принятых мерах прошу проинформировать.

Заместитель начальника начальник Главного следственного управления полковник юстиции

исп.: Щепин А.А.: 573-39-80 (доб. 10127)