



ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
АДМИНИСТРАЦИЯ
ПУШКИНСКОГО РАЙОНА
САНКТ-ПЕТЕРБУРГА

Главам внутригородских
муниципальных образований
Пушкинского района

Октябрьский б-р, 24, Пушкин, Санкт-Петербург, 196601
Телефон: (812) 417-44-47, факс (812) 576-92-21
E-mail: tupush@gov.spb.ru
[http:// www.pushkin.gov.spb.ru](http://www.pushkin.gov.spb.ru)
ОКПО 56309821 ОКОГУ 23010 ОГРН 1027809009755
ИНН/КПП 7820033454/782001001

16.10.2020 № 284-З

На № _____ от _____

Уважаемые коллеги!

Прошу Вас с целью информирования жителей Пушкинского района Санкт-Петербурга о способах преступлений в сфере информационно-телекоммуникационных технологий, связанных с хищениями денежных средств граждан с использованием сети интернет и средств мобильной связи (бесконтактные или дистанционные способы хищений) разместить указанную ниже информацию в октябрьских и ноябрьских выпусках муниципальных СМИ, а также на официальных сайтах муниципальных образований.

В 2020 году произошел резкий рост числа преступлений, связанных с хищениями денежных средств граждан с использованием сети интернет и средств мобильной связи. Жертвами мошенников при совершении хищений в данной сфере становятся наиболее незащищенные слои населения (лица преклонного возраста, пенсионеры, подростки), а также 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 товаров и услуг посредством сети интернет, когда мошенниками используются замаскированные сайты-двойники, посредством которых 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 CVV-кодов.

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 компенсации 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 средства 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.

**Начальник отдела по вопросам законности,
правопорядка и безопасности**



С.Н. Горелов

Скворцов Э.В.
417-44-30