

Памятка

для работников и обучающихся по профилактике и предупреждению дистанционных преступлений в сфере информационно- телекоммуникационных технологий

Это должен знать каждый!

Анализ состояния законности в Санкт-Петербурге показал, что структура преступности претерпела серьезные изменения. При снижении регистрации уличной преступности в целом злоумышленники 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 сфере, 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 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 банковской 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. Персональная страница. Злоумышленники взламывают персональную страницу пользователя в социальных сетях или мессенджерах 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.

Будьте бдительны! Не становитесь жертвами мошенников!