‼️Самые распространенные способы мошенничества в интернете и с мобильного телефона — Будьте внимательны‼️

В Санкт-Петербурге и Ленинградской области участились случаи мошенничества с использованием Интернета и средств мобильной связи — так называемые бесконтактные или дистанционные способы хищений.

Как правило, жертвами мошенников становятся люди преклонного возраста, пенсионеры, подростки, а также люди, не обладающие навыками пользования компьютерными, планшетами, мобильными телефонами.

Наиболее распространенными являются следующие способы хищений:
✅ Мошенничество с банковскими картами — 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 счет, или «угрозе» блокировки банковской карты якобы по причине сбоя в программном обеспечении 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.

✅ Мошенничество «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.

✅ 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.

✅ Мошенничество "Телефонный вирус" — на телефон (на электронную почту) абонента приходит сообщение с просьбой перейти по определенной ссылке, либо предложение установить программу (являющуюся вредоносной) под предлогом зашиты от посягательств на денежные средства. При переходе по ссылке (установке программы) на телефон скачивается «вирус» и происходит списание денежных средств со счета.

✅ 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 тому подобное. 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 внимательны, настороженно и критично относитесь к звонкам незнакомых людей, ни в коем случае не переводите деньги незнакомцам, даже если по телефону вам представляются сотрудниками банков, интернет магазинов, сотрудниками полиции, прокуратуры и другими специалистами! Не устанавливайте неизвестные вам программы на телефон и компьютер!

‼️Будьте бдительными, предупредите друзей и родственников об этих способах мошенничества!