

«Меры предосторожности в сфере информационных технологий»

В последнее время с развитием и использованием информационно-телекоммуникационных технологий наблюдается рост преступлений, совершенных с их использованием.

Посредством Интернета совершаются хищения чужого имущества, осуществляется торговля наркотиками и другие преступления. Среди новых угроз - мошенничества с использованием сотовой связи, а также средств IP-телефонии.

Так, на территории Хабаровского района в текущем году отмечен значительный рост дистанционных мошенничеств. Одной из самых распространенных мошеннических схем является «звонок из службы безопасности банка» и совершение хищения денежных средств под предлогом предотвращения их «списания» с банковского счета гражданина третьими лицами либо активации какой-либо бонусной программы.

Наряду с этим, получил распространение такой вид хищений, как «звонок от лица сотрудников правоохранительных органов». Преступники звонят гражданам, обращаются к ним по фамилии, имени, отчеству, сообщают, что в отношении них либо их близких родственников возбуждено уголовное дело или проводится проверка, в связи с чем возникла необходимость получить данные для аутентификации в системах дистанционного банковского обслуживания, сведения о совершенных по карте операциях или любые другие сведения.

В подобных ситуациях злоумышленники получают персональные данные гражданина, иную конфиденциальную информацию, после чего осуществляют переводы, совершают покупки с его счета в банке. Также имеются случаи, когда потерпевшие самостоятельно перечисляют на счета преступников свои деньги для прекращения уголовного преследования или процессуальной проверки.

Чтобы не стать «жертвой» мошенников, необходимо всегда помнить, что работники банков и правоохранительных органов не выясняют по телефону вопросы о денежных средствах на счетах граждан либо об их банковских картах.

Когда вам звонят и под любым предлогом заводят разговор о финансах, знайте, что это мошенники. При поступлении таких звонков немедленно прерывайте соединение и не ведите разговор со звонящим.

Также по просьбе лиц, позвонивших вам и сообщивших о совершении сомнительных операций, никогда не переводите имеющиеся у вас денежные средства на указанные ими счета, тем более на счета в других банках.

Распространены случаи хищений денежных средств путем оформления онлайн-кредитов при установке гражданами программ удаленного доступа к своим электронным устройствам и передаче прав управления ими третьим лицам.

В преступных целях также используются различные интернет-сервисы для размещения объявлений (Avito, Юла, Drom, BlaBlaCar и другие). Путем введения граждан в заблуждение мошенники становятся владельцами идентификационных данных банковской карты или получают доступ к их личным кабинетам в мобильных банковских приложениях. Указанные действия осуществляются под предлогом перевода средств в счет оплаты товара либо осуществления предоплаты за товар, а также каких-либо услуг по фиктивной доставке товара.

Поэтому, ни при каких обстоятельствах не следует передавать свои технические устройства незнакомым и малознакомым лицам, а при использовании Интернет-ресурсов не переходить по ссылкам на сомнительные сайты.

Не сообщайте указанным лицам свои персональные данные, а также информацию о банковских картах и счетах (номера, коды доступа, пароли и т.д.), не берите по инициативе третьих лиц кредиты на своё имя и не переводите свои денежные средства либо кредитные на счета звонящих вам мошенников, представляющихся сотрудниками правоохранительных органов (прокуратуры, полиции и т.д.), социальных и иных служб, кредитных организаций.

Будьте бдительны при общении по телефону и в сети Интернет.

Информацию подготовила старший помощник прокурора
Хабаровского района Хабаровского края Ильина Ольга Валерьевна