Информация для граждан о способах "обмана на расстоянии". Будьте внимательны

15.08.2019

Сотрудники Отдела уголовного розыска УВД по ЗАО напоминают гражданам о мерах безопасности.

Часть IV.

Сотрудники Отдела уголовного розыска Управления внутренних дел по Западному административному округу сообщают жителям округа о необходимости защиты собственных денежных средств от злоумышленников. Продолжают информировать о разных способах «обмана на расстоянии» и рассказывают о совершенно новой мошеннической схеме завладения вашими деньгами.

Звонок из «банка» с сообщением о попытке снятия денежных средств клиента в другом регионе России.

Как организовано: звонят с неизвестного номера или злоумышленники программными средствами подменяют к определению на телефоне клиента номера банка. Мошенник представляется сотрудником службы безопасности банка и сообщает, что ими только что зафиксирована попытка снятия денег со счета клиента в другом регионе России. Принципиальное отличие данного способа в том, что злоумышленники не просят сообщить им ПИН-код карты и другую персональную информацию! Клиенту рассказывается, что надо определить, с какого конкретно мобильного или стационарного устройства коммуникации, якобы, проходила операция в другом регионе и просят клиента рассказать, на каком устройстве у него установлен банк-клиент, какая версия операционной системы у клиента установлена, IOS или Android. Далее преступник сообщает, что они зафиксировали подключение к системе банк-клиент «лишнего» устройства коммуникации, которое необходимо срочно удалить, и предлагают помочь клиенту это сделать, загрузив на его устройство программу Team-viewer и предоставить всего лишь ID-код этой программы. Важно то, что клиент ни на каком этапе не предоставляет злоумышленникам данные своих счетов или карты и это успокаивает его. После предоставления преступникам ID-кода подключения программы Team-viewer денежные средства выводятся со счета клиента.

На самом деле происходит следующее: Получив ID-код указанной выше программы, преступники получают возможность дистанционного управления аппаратами клиента. И проводят все операции в системе «банк-клиент» самостоятельно, дистанционно, без участия клиента, но с его аппарата. Поскольку злоумышленники полностью имеют доступ к клиентскому входу в банковский сервис, они видят реальные суммы денежных средств клиента и могут полностью очистить все его счета. Опасность для клиента заключается и в том, что впоследствии возвратить ваши деньги будет практически невозможно, поскольку все операции проводятся именно с «клиентского аппарата», а для банка и следственных органов это выглядит, как самостоятельные и осмысленные действия держателя банковской карты,

Ваши действия в подобной ситуации: первое и самое главное правило — прервать разговор. В соответствии с регламентами, разработанными и действующими в каждом банке, есть определенные правила общения с клиентом, и реальные сотрудники банка и его службы безопасности будут только благодарны вашей бдительности и позитивно воспримут ваше желание им перезвонить. Перезванивать следует ИСКЛЮЧИТЕЛЬНО на тот номер телефона, который указан на вашей пластиковой карте. Перезвонив самостоятельно в банк, вы можете уточнить, был ли реальный звонок из банка, есть ли в действительности опасность для сохранности ваших денежных средств. Что бы вам не говорили, прерывайте разговор и берите инициативу в свои руки.

Ваша бдительность поможет вам сохранить ваши накопления и обеспечить вашу финансовую безопасность.
