

Дистанционное мошенничество. Новые схемы обмана.

Важнейшая проблема, с которой сталкиваются многие граждане – это дистанционное мошенничество, связанное с получением мошенниками удаленного доступа к банковской карте и интернет-мошенничеством. Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов», «подключения к социальной программе» или иных надуманных предлогов злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

В настоящее время получают распространение и иные схемы дистанционного мошенничества.

Злоумышленники звонят под видом сотрудников страховых компаний и сообщают о необходимости продления полиса ОМС. Для дистанционного обновления предлагают скачать приложение Минздрава, которое на самом деле фейковое и позволяет получить удаленный доступ к смартфону, а также интернет-банку и portalу «Госуслуги». Если поступил такой звонок, незамедлительно прекращайте разговор и перезвоните в службу поддержки вашей страховой компании, чтобы уточнить всю необходимую информацию.

Также мошенники могут позвонить человеку по телефону или через мессенджер и сообщить, что его денежные средства якобы пытаются похитить, а для решения проблемы по «хищению» необходимо установить приложение Центрального Банка Российской Федерации, которое является фейковым. Затем злоумышленники просят запустить приложение и ввести код подтверждения от банка якобы для авторизации. Именно так мошенники получают необходимые им данные карты.

Приложение, которое просят установить мошенники, создаёт виртуальный образ банковской карты жертвы, который злоумышленники используют для снятия денежных средств в банкоматах, поддерживающих бесконтактную технологию.

Таким образом, вместо банковской карты человека мошенник прикладывает к банкомату свой смартфон.

Не скачивайте приложения по просьбе незнакомых людей и не сообщайте никому свои персональные данные!