

 **ОМВД России по Челябинской области информирует о появлении новых видов мошенничеств, совершаемых с использованием IT-технологий:**

! Сайты, имитирующие ресурсы государственных ведомств и справочных систем. Мошенники размещают шаблоны документов, которые обычно ищут в интернете бухгалтеры, секретари, или другие сотрудники, занимающиеся налоговой или финансовой деятельностью. Шаблоны документов при этом заражены вирусами. Когда сотрудник скачивает документ, на его компьютере запускается программа удаленного доступа. С ее помощью мошенники меняют в договорах компании банковские реквизиты, чтобы получить на свои счета деньги, предназначенные подрядчикам и заказчикам.

! Мошенники представляются сотрудниками банка предлагают установить на смартфон "официальное сертифицированное" приложение финансовой организации для проверки устройства и поиска уязвимостей. Далее злоумышленники отправляют потенциальным жертвам ссылку на фишинговый сайт с инструкцией по установке приложения. После установки приложения мошенники получают удаленный доступ к смартфону и выводят денежные средства из онлайн банка клиента.

! Сообщения от якобы Федеральной службы судебных приставов. Мошенники направляют гражданам электронные письма и сообщения об имеющейся задолженности, угрожая внести должника в "федеральный реестр недобросовестных плательщиков", заблокировать его счета (банковские карты). Чтобы избежать этого, необходимо по поступившей ссылке для погашения имеющейся задолженности. После перехода по ссылке, денежные средства перечисляются на счета мошенников

 Если же вы пострадали от мошенничества, следует немедленно обратиться в отделение полиции по телефону 02, 2-02-02 дежурной части.

[#полицияЮжногоУрала](#) [#мошенничество](#) [#Катав](#) [#южныйурал](#) [#законипорядок](#) [#челябинскаяобласть](#) [#отделполиции](#) [#mvd74](#) [#будьтевнимательны](#) [#профилактика](#) [#остановиммошенника](#) [#акция](#)

[#Внимание](#) [#ОсторожноМошенники](#) [#НеДайСебяОбмануть](#)

