

УМВД России по Приморскому району предупреждает:

НИКОГДА НЕ СООБЩАЙТЕ ПО ТЕЛЕФОНУ ДАННЫЕ СВОЕГО ПАСПОРТА, НОМЕР СНИЛС, СМС-СООБЩЕНИЯ С КОДОМ!

При поступлении подозрительных звонков прекратите разговор и сообщите о случившемся в полицию по телефону **02** или **112**

УКРАСТЬ ВАШИ ДЕНЬГИ пытаются так:

Злоумышленники представляются сотрудниками Пенсионного фонда России и сообщают, что у вас имеется неучтенный стаж работы - необходимо подъехать в здание фонда и произвести перерасчет. Однако предварительно надо записаться на прием - с этой целью мошенники просят сообщить им номер СНИЛС либо паспорта. После этого ваши персональные данные могут использоваться в противоправных целях, для оформления кредита в микрофинансовых организациях.

ПОМНИТЕ, что с 1 января 2023 года начал работу Социальный фонд России, который объединил Пенсионный фонд и фонд социального страхования.

Представители государственных органов звонят только в случае вашего обращения к ним и никогда не спрашивают данные паспорта, номер СНИЛС и прочих документов.

Злоумышленники представляются сотрудниками военной прокуратуры и просят сообщить им данные паспорта либо сберкнижки, после чего получают доступ к денежным средствам граждан, хранящихся на банковских счетах, либо оформляют от их имени кредиты в микрофинансовых организациях и используют денежные средства в противоправных целях.

ПОМНИТЕ: сотрудники органов прокуратуры, в том числе военной, звонят гражданам только в случае их обращения к ним либо в случае необходимости явки гражданина для получения объяснения по проводимой проверке.

По электронной почте поступает сообщение о взломе аккаунта Госуслуг и утечке персональных данных пользователей с предложением связаться с сотрудниками Минцифры, ФСБ или технической поддержки. При наборе предложенного номера телефона гражданин узнает, например, о том, что мошенники уже подали заявку на оформление кредита от его имени.

Чтобы их опередить, предлагают срочно самому оформить на себя кредит, а полученные деньги перевести на «безопасный счет».

ПОМНИТЕ: при получении такого сообщения необходимо самостоятельно зайти на сайт Госуслуг и удостовериться, что с аккаунтом все в порядке.

Мошенники создают аккаунт в мессенджерах WhatsApp, Telegram, визуально похожий на аккаунт руководителя. С него работникам организации направляют сообщение о необходимости связаться, например, с сотрудником полиции. Те, кто верит и звонит, узнают о попытке хищения денег со счета или переводе на счет террористической организации - этому можно противодействовать, переведя деньги на «безопасный счет».

То же самое делают при помощи сгенерированного с помощью искусственного интеллекта голоса руководителя, направляя работникам подобные голосовые сообщения при помощи тех же мессенджеров.

ИСКЛЮЧИТЕ НЕМЕДЛЕННОЕ ВЫПОЛНЕНИЕ ПРОСЬБЫ! Позвоните своему руководителю по имеющимся у вас контактам и проверьте информацию.