

Уважаемые коллеги!

Обращаем внимание на участившиеся случаи мошенничества путем совершения звонков по телефону и отправки сообщений в интернет-мессенджерах (WhatsApp, Telegram) от имени известных вам лиц (руководителей и сотрудников научных учреждений) с использованием программных средств для подмены номера и имитации голоса. Как правило, обращение содержит просьбу оказать содействие сотрудникам правоохранительных органов (ФСБ, МВД, Следственный комитет, прокуратура) и иных структур (Центробанк России, Росфинмониторинг, органы власти и т.п.) в расследовании преступления. После чего к вам могут обратиться, в том числе по видеосвязи, мнимые представители вышеуказанных ведомств. В ходе переговоров злоумышленники настойчиво могут убеждать вас в том, что с ваших банковских счетов фиксируются попытки хищения денежных средств для финансирования ВСУ. В целях пресечения «противоправной» деятельности предлагается перевести деньги на безопасные счета.

Также фиксируются случаи совершения звонков от имени государственных учреждений, банков, мобильных операторов и организаций, оказывающих различные услуги. Их целью является получение доступа к личным кабинетам на портале «Госуслуги» и в мобильных приложениях банков. Мошенники просят продиктовать направленный на ваш телефон код, необходимый для авторизации или регистрации. Получив удаленный доступ, злоумышленники могут похитить ваши сбережения и оформить кредиты.

Признаками действий телефонных мошенников являются:

- настойчивость при общении;
- убеждение в необходимости принятия срочных действий;
- отказ на просьбы перезвонить для проверки информации или привлечь к разговору кого-либо из ваших родственников, знакомых иных лиц для внесения ясности;
- участие в разговоре сотрудников силовых и иных структур (ФСБ, МВД, Следственный комитет, Центробанк России и т.п.);
- требование о неразглашении факта оказания содействия правоохранительным органам;
- необходимость строгого соблюдения доводимых инструкций;
- оказание психологического давления путем доведения до информации о переводе ваших средств на счета террористических и экстремистских организаций, финансировании вооруженных формирований Украины и угроз

привлечения вас к уголовной ответственности за соучастие в указанных преступлениях;

- отказ от личного общения в учреждениях, сотрудниками которых представляются.

Во избежание совершения в отношении вас мошеннических действий, необходимо прекратить телефонный разговор с мнимыми сотрудниками. Необходимо знать, что переводы денежных средств, совершенные от вашего имени, возврату не подлежат. Коды доступа в личные кабинеты, полученные мошенниками, сразу используются ими для входа и смены прав доступа с целью совершения операций от вашего имени.

В случае совершения в отношении вас мошенничества и наличия признаков доступа к вашим персональным данным в личном кабинете на портале «Госуслуги» или приложениях банков, следует незамедлительно обратиться в МФЦ и банковские учреждения в целях предотвращения финансовых операций от вашего имени. Сообщите о преступлении в правоохранительные органы.

Пострадавших от телефонных мошенников спецслужбы Украины могут склонять к совершению на территории РФ преступлений (диверсии, террористические акты) для возвращения денежных средств. При получении подобных предложений следует незамедлительно обратиться в правоохранительные органы (МВД, ФСБ России).

О мерах безопасности при общении по телефону необходимо проинструктировать персонал.