Опасайтесь мошенников!

В настоящее время все чаще в мошеннических целях в социальных сетях и мессенджерах используются поддельные («зеркальные») аккаунты руководителей органов государственной власти, а также других известных лиц. Такие аккаунты содержат реальные данные руководителей организаций (фамилия, имя, отчество, фото и т.п.) и выглядят максимально достоверно.

Злоумышленники действуют примерно по сходным сценариям. Например, сотрудник организации получает сообщение в социальной сети, мессенджере или по электронной почте, якобы, от своего руководителя. При этом злоумышленник обращается к сотруднику, используя его имя и отчество, чтобы вызвать доверие. В процессе общения мошенник предупреждает о последующем телефонном звонке из какой-либо организации или правоохранительных органов и просит сотрудника никому об этом не сообщать, а после завершения - отчитаться о результатах разговора. После этого сотруднику организации поступает звонок, в ходе телефонного разговора у сотрудника запрашивается конфиденциальная информация, также его вынуждают совершить определенные действия, как правило, направленные на отчуждение денежных средств в пользу злоумышленников.

Ещё одной из мошеннических схем является рассылка в социальных сетях и мессенджерах сообщений с предложением проголосовать по различным темам (участие в конкурсе, выбор музыкальной композиции, фильма и т.п.), содержащих ссылку, после перехода по которой легальный аккаунт пользователя перехватывается злоумышленниками.

Кроме этого, мошенники стали выдавать себя за сотовых операторов, требуя продлить договор на номер.

Телефонные мошенники обзванивают абонентов под видом сотовых операторов с предложением продлить якобы истекающий договор на номер телефона. Во время разговора злоумышленник старается отвлечь внимание собеседника обилием технических деталей, после чего уточняет, на какой период клиент желает продлить контракт с оператором. Затем на номер абонента приходит сообщение с кодом, которое необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок». Тем временем телефонный мошенник продолжает отвлекать собеседника различными мелкими деталями, пока не спрашивает цифры и код, полученные в сообщении. Затем злоумышленник сообщает, что направил клиенту ссылку, где необходимо ввести код «для завершения дистанционного подписания пользовательского соглашения».

Однако этот код не что иное, как данные для входа в личный кабинет жертвы на портале Госуслуг. Надо помнить, что договоры, заключаемые абонентом с сотовыми операторами, не предусматривают ограниченного срока пользования номером.

Будьте бдительны и не поддавайтесь на уловки мошенников!

Зачастую для того, чтобы усыпить бдительность граждан, мошенники представляются сотрудниками Следственного комитета, при этом подменяя реальный телефонный номер на номера телефонов следственного управления.

Напоминаем, что сотрудники Следственного комитета никогда не требует по телефону предоставления персональных данных и банковских реквизитов, информации по счетам и пластиковым картам. В случае поступления таких незаконных требований и предложений от имени сотрудников Следственного комитета, просим немедленно сообщать об этом по телефону доверия регионального следственного управления 395-506 (круглосуточно).

При выявлении действий мошеннического характера, в случае поступления звонка с просьбой назвать свои личные данные, номер карты или счета, или перевести деньги, следуя инструкциям со стороны звонящего, необходимо сразу же завершить разговор и обратиться в полицию.

Будьте бдительны, чтобы не стать жертвой мошенников!

01 Декабря 2023

Адрес страницы: https://omsk.sledcom.ru/news/item/1842865