Автор: Administrator
17.01.2024 13:55 -

Кольчугинская межрайонная прокуратура информирует граждан о мошеннических действиях в социальных сетях и мессенджерах

В настоящее время выявлены многочисленные факты использования в мошеннических целях в социальных сетях и мессенджерах поддельных («зеркальных») аккаунтов руководителей органов государственной власти федерального, регионального и муниципального уровней, предприятий оборонно-промышленного комплекса (далее организации), а также руководителей подразделений Банка России.

Во всех случаях преступники действуют примерно со сходными сценариями. Сотрудник организации получает сообщение в социальной сети, мессенджерах для связи с сотрудниками организации. Указанные аккаунты содержат реальные данные руководителей (фамилия, имя отчество, фото) которые выглядят максимально достоверно.

В процессе общения злоумышленник предупреждает о последующем телефонном звонке из какой-либо организации никому о нем не сообщать, а после завершения - отчитаться о результатах разговора.

После этого сотруднику организации поступает звонок, в ходе которого у него могут запрашивать различную конфиденциальную информацию и вынуждать совершать противоправные действия в пользу злоумышленников.

Продолжая совершенствовать методы социальной инженерии злоумышленники в ряде случаев проводят предварительную разведку и используют информацию о потенциальных жертвах, чтобы вызвать доверие. В приведённом примере злоумышленники используют доверие сотрудников организаций к непосредственному руководителю и страх столкнуться с последствиями отказа выполнить его требования. Подобным «атакам» уже подверглись работники государственных организаций, организаций оборонно-промышленного комплекса и потребительского сегмента бизнеса.

С поддельных аккаунтов злоумышленниками рассылаются сообщения также и в адрес

руководителей и работников других организаций с целью получения контактных данных лиц, необходимых мошенникам для дальнейшего взаимодействия и совершения противоправных действий.

Ещё одной из распространённых 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. В этом случае необходимо при восстановлении доступа к аккаунту использовать штатные механизмы социальной сети и мессенджера.

Дополнительно обращаем внимание, что работники Банка России для решения рабочих вопросов используют исключительно официальные каналы связи.

Если все-таки мошенникам удалось совершить преступление, то жертве необходимо обратиться в полицию с заявлением или по телефону 112, сохранить ссылки на сайты, с которых были совершены мошеннические действия, переписку с мошенниками и другие данные, которые могут быть полезны для идентификации мошенника.