О мошеннических действиях, совершаемых 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. Указанные аккаунты содержат реальные данные руководителей (фамилия, имя, отчество, фото) и выглядят максимально достоверно. **Злоумышленники используют эти поддельные аккаунты в социальных сетях и мессенджерах для связи с сотрудниками организаций.**

Во всех случаях преступники действуют примерно по сходным сценариям. 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 злоумышленник предупреждает о последующем телефонном звонке из какой-либо организации или правоохранительных органов, **просит сотрудника организации оказать необходимое содействие, никому не сообщать о разговоре, а после завершения – отчитаться о результатах.**

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 злоумышленники рассылают 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.). Эти сообщения содержат 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.

Совершаемые злоумышленниками неправомерные действия могут нанести репутационный ущерб органам власти, в том числе снизить уровень доверия граждан к ним.