ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Дальневосточное главное управление
Отделение по Магаданской области
685000, г. Магадан, ул. Пушкина,4
Тел. (413 2) 695304, факс 695305
44magadan@cbr.ru

Губернатору
Магаданской области

С.К. Носову

От 03.11.2023 № Т744-12-5/3234

на от

О мошеннических действиях в социальных сетях и мессенджерах

Уважаемый Сергей Константинович!

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.

Одной из распространённых схем является использование злоумышленниками поддельных аккаунтов в социальных сетях и мессенджерах для связи с сотрудниками организаций. Указанные аккаунты содержат реальные данные руководителей (фамилия, имя, отчество, фото и т.п.) и выглядят максимально достоверно.

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 и просит сотрудника 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, а также руководители подразделений Банка России.

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.

Совершаемые злоумышленниками неправомерные действия могут повлечь следующие негативные последствия:

- нанесение репутационного ущерба Банку России и организациям;
- снижение уровня доверия граждан к финансовым услугам.

Считаем необходимым довести изложенную информацию до подчинённых работников в целях предотвращения возможности совершения в отношении них мошеннических действий.

При выявлении действий мошеннического характера предлагаем незамедлительно обращаться в территориальные подразделения органов внутренних дел, а также сообщать о них в Банк России.

Кроме того, сообщаем, что работники Банка России для решения рабочих вопросов используют исключительно официальные каналы связи.

И.о. управляющего Отделением Магадан С.С. Пудровский

Банк России
ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 40:60:1D:00:0D:9F:00:FA:82:14:14:97:64:AB:9F:CE
Владелец **Пудровский Станислав Станиславович**
Действителен с 10.07.2023 по 30.08.2036

Е.Ю. Соколов
695326