

**ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

**Волго-Вятское главное управление
Отделение – Национальный банк
по Республике Мордовия**

Главе муниципального района
Республики Мордовия
(по списку рассылки)

Мордовия Республикасо Национальной банконь башка пияльксесь	Мордовия Республикасо Национальной банконь башка пияльксесь
---	---

430005, г. Саранск, ул. Коммунистическая, 32Б
www.cbr.ru

от 31.10.2023 № Т489-9-5/3504
на № _____ от _____

О мошеннических действиях в социальных
сетях и мессенджерах

В целях повышения уровня осведомленности о схемах, используемых при совершении мошеннических действий в социальных сетях и мессенджерах, Отделение – Национальный банк по Республике Мордовия Волго-Вятского главного управления Банка России сообщает, что Банком России выявлены многочисленные факты использования в мошеннических целях поддельных («зеркальных») аккаунтов руководителей органов государственной власти федерального, регионального и муниципального уровней, предприятий оборонно-промышленного комплекса, 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 органам государственной власти и организациям;

снижение уровня доверия граждан к финансовым услугам.

Также информируем, что работники Банка России для решения рабочих вопросов используют исключительно официальные каналы связи.

В целях предотвращения возможности совершения мошеннических действий предлагаем довести данную информацию до подчиненных сотрудников, а также подведомственных учреждений и организаций.

И.о. управляющего

Отделением-НБ Республика Мордовия



В.П. Быстров