ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Южное главное управление
Отделение по Ростовской области

344006, г. Ростов-на-Дону,
просп. Соколова, 22а
www.cbr.ru
тел. (863) 263-93-83 /факс (863) 263-93-09

Министерствам, ведомствам,
муниципальным образованиям
Ростовской области

(по списку рассылки)

От

на № от

О мошеннических действиях
в социальных сетях и мессенджерах

Банком России уделяется повышенное внимание вопросам обеспечения безопасности финансовых услуг, оказываемых населению и организациям, в сотрудничестве с правоохранительными и иными органами государственной власти проводится системная работа по профилактике и противодействию преступлениям и правонарушениям в кредитно-финансовой сфере.

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 распространенных 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 приведенном 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.

Еще одной из распространенных 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.

Информируем о вышеизложенном в целях повышения уровня информационной безопасности, при выявлении подобных случаев просим сообщать о них в Банк России (сайт Банка России – www.cbr.ru, раздел «Интернет-приемная»).

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

Благодарим за сотрудничество!

Управляющий
Отделением Ростов-на-Дону Н.Н. Леонтьева

В.В. Изотов
тел.: (863) 261-39-23