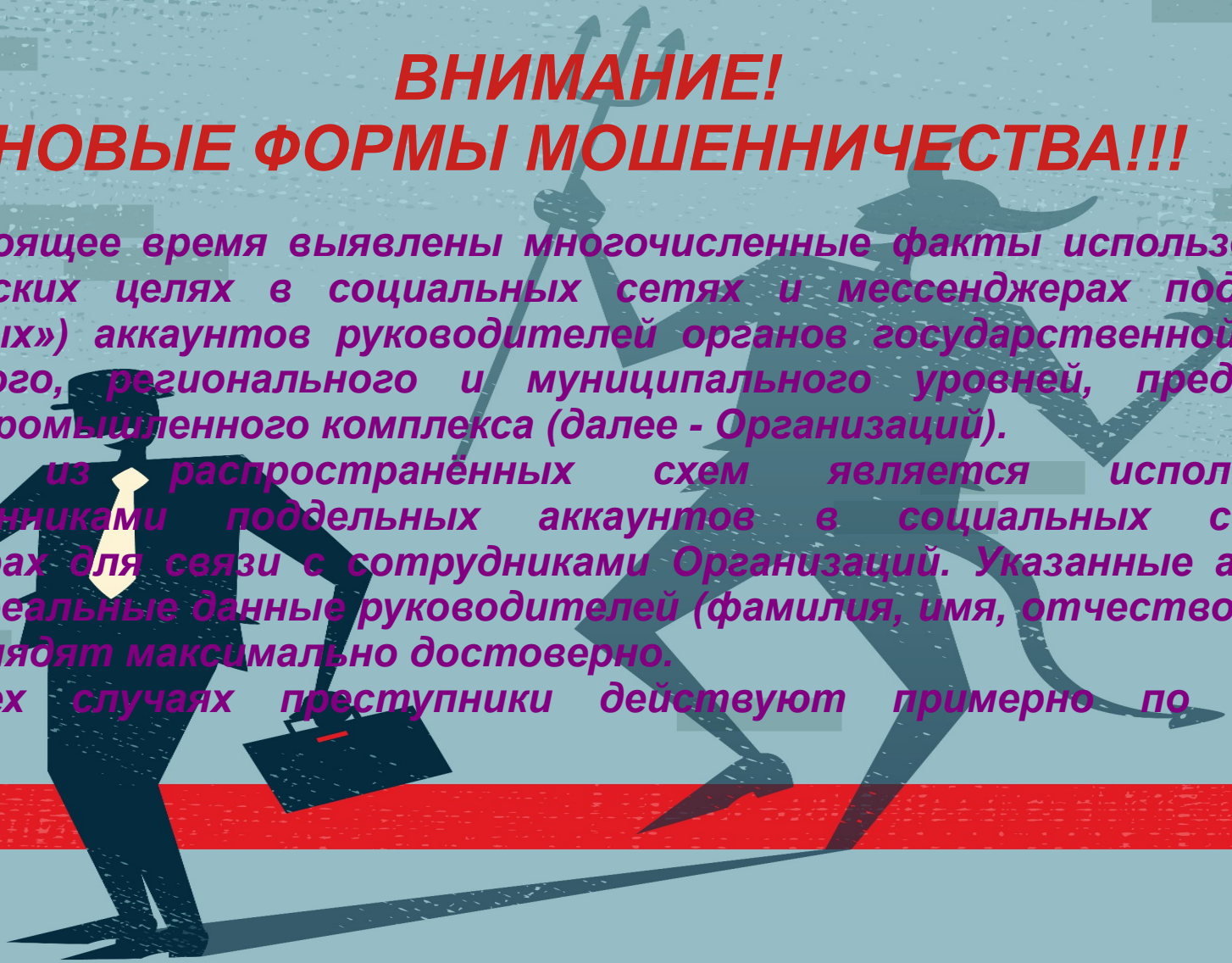
ВНИМАНИЕ!
НОВЫЕ ФОРМЫ МОШЕННИЧЕСТВА!!!



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 - Организаций).

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:

1 сценарий:

- 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;

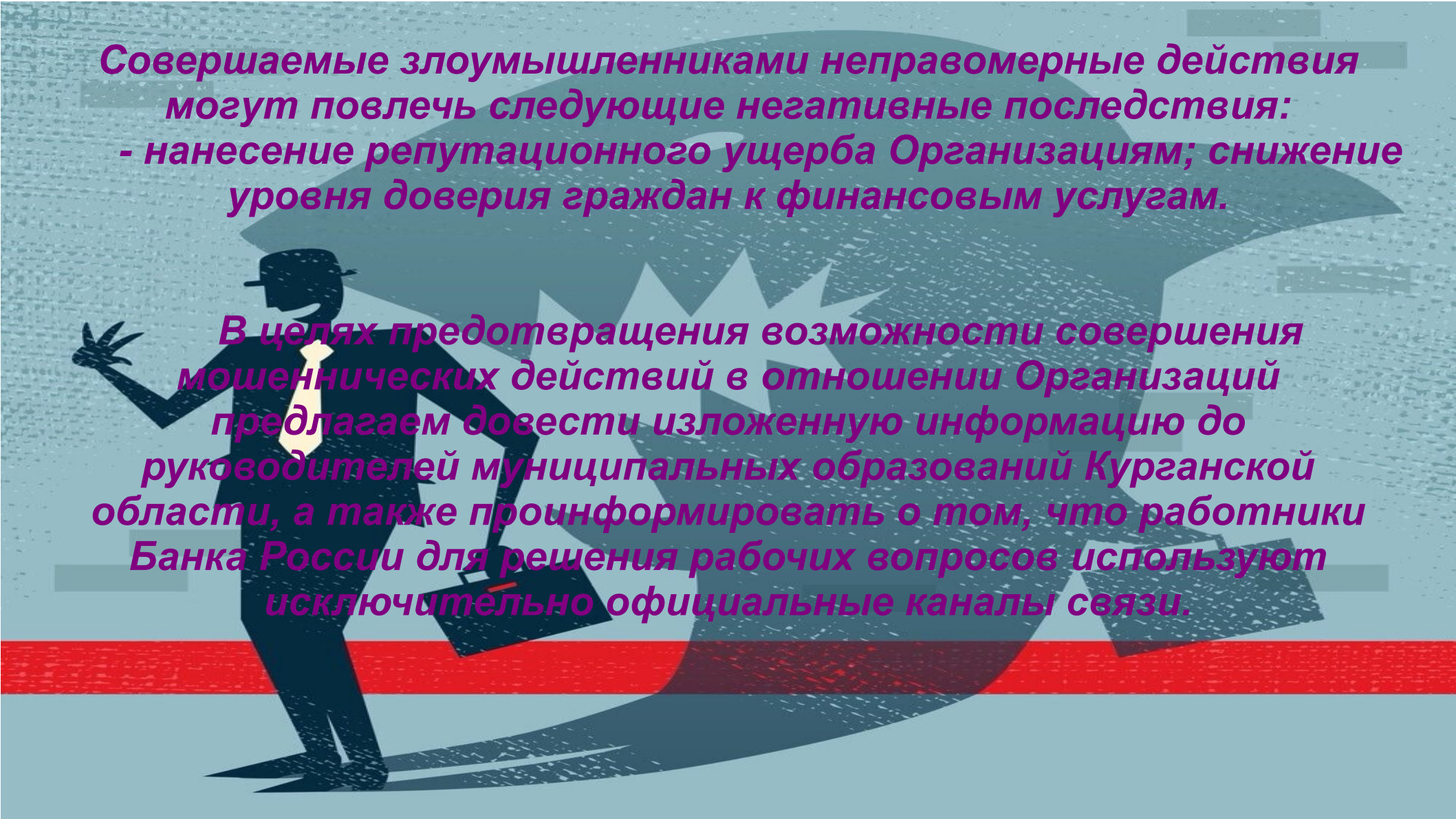
- после этого сотруднику Организации поступает звонок, в ходе которого у него могут запрашивать различную конфиденциальную информацию и вынуждать совершать противоправные действия в пользу злоумышленников;

- 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.

- 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.

2 сценарий:

- 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 Организациям; снижение уровня доверия граждан к финансовым услугам.

В целях предотвращения возможности совершения мошеннических действий в отношении Организаций предлагаем довести изложенную информацию до руководителей муниципальных образований Курганской области, а также проинформировать о том, что работники Банка России для решения рабочих вопросов используют исключительно официальные каналы связи.