КОНСПЕКТ
по профилактике и пресечению мошенничеств, совершаемых по схеме «Fake boss» («Лжеруководитель»)

В современных условиях отмечается трансформация способов совершения противоправных деяний в сфере высоких технологий. Наряду с традиционными методами хищения денежных средств (фишинг, несанкционированный доступ к учетным записям устройств Apple, обман под предлогом перерасчета пенсий, замены приборов учета, инвестирования и т.д.), злоумышленники активно применяют многоуровневую схему «Fake boss» (мошенничество от имени руководителей организаций и ведомств).

1. Характеристика и этапы реализации схемы.

Реализация преступного замысла носит спланированный характер и включает в себя следующие этапы.

Подготовительный этап: сбор и систематизация персональных данных руководителей и работников учреждений и предприятий (ФИО, занимаемые должности, контактные телефоны, структура подчиненности) из открытых источников или в результате компрометации учетных записей мессенджеров (например, посредством фишинговых рассылок под видом голосования в конкурсах).

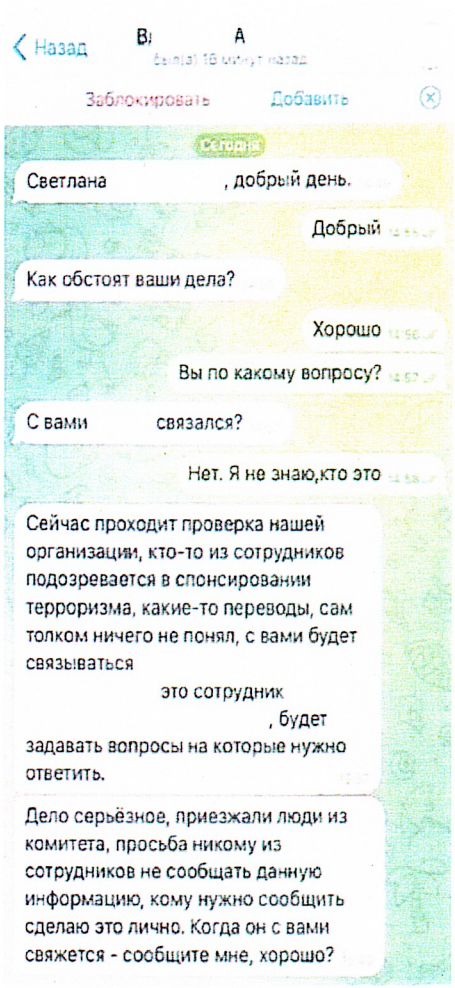
Инициализация контакта: создание злоумышленниками поддельных (фейковых) аккаунтов в мессенджерах с использованием персональных данных и фотоматериалов руководителей организаций либо структурных подразделений.

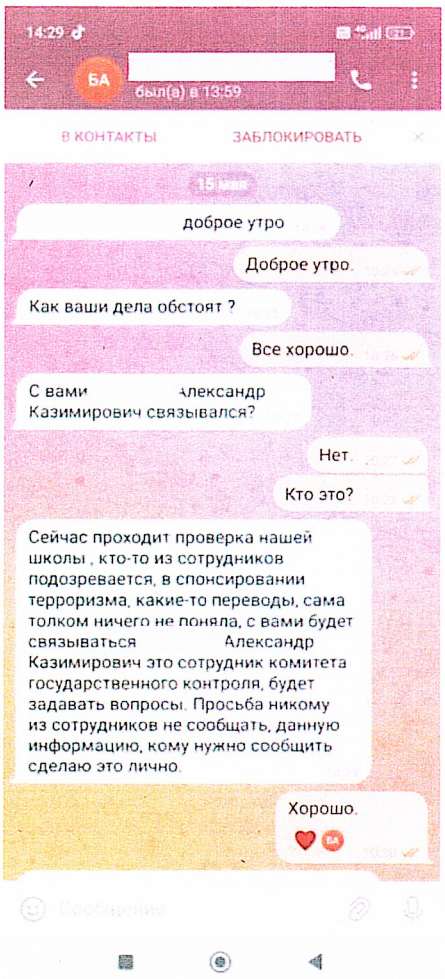
Психологическое воздействие и дезинформация: от имени «руководителя» с подчиненным устанавливается диалог (текстовые сообщения, реже – сгенерированные с помощью нейросетей голосовые или видеосообщения). Подчиненному сообщается о якобы проводимой контрольными или правоохранительными органами проверке, выявленных чрезвычайных происшествиях, подозрении в пособничестве экстремистской деятельности либо угрозе привлечения к уголовной ответственности.

Принуждение к противоправным действиям: под предлогом «спасения средств предприятия», «сохранения конфиденциальности» или «участия в специальной операции» работника убеждают перечислить личные сбережения либо средства организации на «безопасный счет», либо передать их наличными курьеру. Злоумышленники используют методы жесткого психологического давления, ограничение по времени на принятие решений и запрет на обсуждение ситуации с коллегами и родственниками.

Завершающий этап: после завладения денежными средствами переписка в мессенджерах оперативно удаляется, а связь с потерпевшим прекращается.

2. Типичный пример реализации схемы (скриншот переписки в мессенджере).





Пример сообщения: «Сейчас проходит проверка нашей школы, кто-то из сотрудников подозревается в спонсировании терроризма... с вами будет связываться сотрудник Комитета государственного контроля... Просьба никому из сотрудников не сообщать, данную информацию кому нужно сообщу сам лично».

Данный пример демонстрирует классическое использование административного давления, запугивание тяжкими обвинениями (финансирование терроризма) и введение режима строгой конфиденциальности с целью изоляции жертвы от внешних источников помощи и критического мышления.

Кроме того, в рамках схемы «Fake boss» злоумышленники от имени руководителей или коллег могут направлять сообщения с просьбой одолжить денег или срочно перевести финансовые средства на указанные реквизиты под различными предлогами (например, необходимость срочной оплаты закупки, закрытия непредвиденных расходов по работе при заблокированных счетах, участия в экстренном сборе или помощи в сложной личной ситуации). Подобные обращения также сопровождаются

требованием строгой конфиденциальности, запретом обсуждать происходящее с кем-либо и искусственно создаваемой атмосферой спешки.

3. Алгоритм действий при совершении противоправных деяний.

Прекратить коммуникацию: немедленно остановить переписку и телефонный разговор с подозрительным «руководителем» или представляющимися «правоохранителями» лицами.

Проверить информацию: связаться с руководством или коллегами через официальные, проверенные ранее контакты (напрямую по внутреннему или рабочему номеру).

Обратиться в правоохранительные органы: в случае совершения мошеннических действий и перечисления денежных средств необходимо незамедлительно обратиться в ближайший орган внутренних дел (или позвонить по номеру 102) для блокирования транзакций и проведения оперативно-розыскных мероприятий.

Главное управление по противодействию киберпреступности
криминальной милиции МВД Республики Беларусь