АО УКБ «Белгородсоцбанк» предупреждает о **значительном росте мошеннических атак** в мессенджерах и по телефону. Злоумышленники маскируются под руководителей компаний, создавая дублирующие аккаунты и используя их авторитет для обмана.
Цель мошенников — под предлогом срочного вопроса или просьбы перезвонить войти в доверие и совершить обманные действия (получение конфиденциальных данных, перевод денежных средств и т.п.).

Как действуют мошенники?

Сценарии атак строятся на методах **социальной инженерии** и включают несколько этапов:

1. Создание легенды

Мошенники создают в мессенджерах фейковый аккаунт, используя фотографию и реальные данные руководителя компании. Номер телефона при этом может быть скрыт. Сам руководитель не теряет контроль над своим основным аккаунтом.

2. «Кредит доверия»

Для придания правдоподобности мошенники совершают первый звонок с «плохой слышимостью», чтобы переместить общение в мессенджер.

- **Сотрудникам** сообщают о проведении проверки с участием правоохранительных органов.
- **Клиентам** пишут о необходимости срочно уточнить важный вопрос.

3. Атака

Спустя некоторое время звонок поступает уже от имени «службы безопасности» или «топ-менеджера». Для усиления давления может использоваться видеозвонок, где с помощью технологий искусственного интеллекта (дипфейк) генерируется изображение реального руководителя.

Что делать? Рекомендации Банка

При любых подозрительных звонках или сообщениях следуйте простым правилам:

☑ **Проверяйте отправителя**

Обратите внимание на номер телефона, дату создания аккаунта, недавние изменения фото или имени в профиле.

☑ **Анализируйте детали**

Необычное приветствие, нестандартные требования, искусственная спешка или требование секретности — явные признаки мошенничества.

☑ **Никогда не передавайте** пароли;

- PIN-коды;
- CVC/CVV-коды карт;
- SMS- или push-коды подтверждения.

☑ **Не открывайте вложения и не переходите по ссылкам** от сомнительных контактов — они могут содержать вредоносное ПО.

☑ **Перезванивайте по проверенному каналу связи**

Если сообщение или звонок вызывают сомнения — прервите разговор и свяжитесь с человеком по номеру, который известен вам ранее (рабочий телефон, официальный адрес электронной почты).

«Банк фиксирует рост числа попыток обмана, когда мошенники выдают себя за руководителей компаний или партнёров. Они играют на доверии к авторитету и создают искусственную срочность с элементами секретности, чтобы заставить человека действовать быстро, не успев критически оценить ситуацию. Новые технологии, включая искусственный интеллект, делают эти атаки всё более правдоподобными — от поддельных голосов до убедительных видео. Призываем сохранять „холодную голову“ и всегда перепроверять информацию, особенно если собеседник пишет с нового аккаунта».

Будьте бдительны!

Если вы столкнулись с подозрительной активностью — незамедлительно сообщите в Банк по официальным каналам связи.