

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БИОМЕТРИИ



Биометрические технологии позволяют быстро и удобно подтвердить личность, но их использование связано с рисками кражи данных.

Мошенники охотятся за фотографиями, видео- и аудиозаписями пользователей. Похищенные биометрические данные используются для обхода систем аутентификации — и хищения денежных средств через подложные операции.

ВАЖНО!

Помните, что внешность человека, его голос и другие характеристики, используемые для биометрической аутентификации, публично доступны, и не могут быть произвольно изменены. Это отличает их от паролей. Поэтому биометрия не должна использоваться как основной метод идентификации пользователя.



СЛЕДУЙТЕ НЕСКОЛЬКИМ ПРАВИЛАМ:



1 Установите уникальный и надёжный пароль для входа в приложение и личный кабинет клиента банка. Регулярно меняйте его



2 Используйте дополнительные методы аутентификации, такие как вход по SMS / Push-уведомлению



3 Сохраняйте бдительность при подозрительных звонках — особенно, если собеседник настойчиво добивается, чтобы вы произнесли определённые слова или фразы



4 Если мошенники представляются сотрудниками банка и просят сдать биометрические данные по телефону, прервите разговор и обратитесь в колл-центр вашего банка самостоятельно



5 Установите ограничение на сумму переводов и снятия денег, а также используйте для подтверждения операций несколько видов защиты — с помощью одноразового пароля или кодового слова

Что делать, если вы подозреваете, что ваши биометрические данные украдены?



- 1 Отключите подтверждение личности с помощью биометрии в тех системах, где она была включена, и перейдите на другие методы входа.
- 2 Обратитесь в службу поддержки биометрической системы.
- 3 Если мошенники сняли деньги с вашей карты, напишите заявление в ближайшем отделении полиции.

Биометрия может быть очень удобным и достаточно надёжным способом аутентификации пользователя, если соблюдать простые правила и не терять бдительность.

Главное, помните: биометрия не должна быть единственным методом защиты ваших учётных записей, особенно в ситуациях, когда речь идёт о важных данных или финансовых операциях.