Что такое биометрические данные и в чем их главная угроза?

Биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (отпечатки пальца, геометрия лица, голос и иное).

Угроза кражи биометрических данных – это угроза вашей идентичности, репутации и приватности в долгосрочной перспективе.

В настоящее время мошенники в основном собирают фотографии и голоса россиян.

Как мошенники использую собранные данные:

1. Чтобы создавать дипфейки для обмана близких, друзей и коллег. Мошенники создают правдоподобные легенды и, в конечном итоге, выманивают у жертвы деньги.
2. Кража аккаунтов. Некоторые сервисы требуют подтверждения личности по видео. Получив нужные ракурсы лица, мошенники проходят такие проверки.
3. Фальшивые профили и документы. Фотографии используют для создания поддельных аккаунтов в соцсетях, схем с «Fake boss» (поддельный руководитель) или фиктивных анкет на вакансию.
4. Шантаж и дескридитация. Данные могут попасть в открытый доступ или продаваться на теневых форумах. Это риск репутационных потерь.

Для сбора биометрических данных злоумышленники могут:

- совершать вам звонки по видеосвязи и во время общения вести видеозапись разговора;
- рассылать массовые сообщения, как правило, со ссылкой на фишинговые (поддельные) сервисы, к примеру, якобы «Госуслуги», банковский сервис или интересное приложение, и под предлогом оплаты услуги или составления заявки требовать подтвердить личность: включить камеру и показать лицо со всех ракурсов или, глядя в камеру, помахать рукой;
- собирать ваши фотографии и видео из социальных сетей, где вы выложили их с открытым доступом.

Следует отметить, что запись видео с лицом гражданина не позволяет получить доступ к банковским приложениям и платежным средствам. Российские банковские биометрические сервисы устойчивы к дипфейкам, даже если они сделаны на основе собранных данных по таким сценариям. Недостаточно для успешной идентификации и простой записи голоса.

В то же время в настоящее время уже зафиксировано, что биометрические данные активно используются злоумышленниками как инструмент психологической манипуляции после взаимодействия российских граждан с фишинговым (поддельным) ресурсом.

Пользуясь тем, что данный способ верификации относительно новый, мошенники активно применяют сообщения о взломе или утечке биометрических

данных в схемах, предполагающих инициативный звонок гражданина в поддельную техническую поддержку.

Так, в Республике Башкортостан заявителю после взаимодействия с фишинговым (поддельным) ресурсом поступило уведомление «Вы успешно подтвердили вход с помощью биометрии по фото с нового устройства Айфон 14 Про Макс. Выгрузка данных запущена, по окончанию отчет будет отправлен на почту mamontscam1312@yandex.ru». После чего с ним связался неизвестный и, представившись сотрудником портала «Госуслуги», под предлогом обеспечения безопасности денежных средств, путем обмана похитил 500 000 рублей и 1 200 долларов.

Несмотря на отсутствие фактов применения биометрических данных для неправомерного доступа к платежным сервисам, необходимо соблюдать базовые меры безопасности.

Принципы финансовой самообороны с приходом новых технологий не меняются.

Никто из официальных лиц (банк, госорганы) не будут запрашивать биометрию (видео с лицом и голосом) по телефону или через смс-рассылку. Поскольку процесс сбора биометрии проходит в строго регламентированном порядке. Единственный безопасный способ сдать свои биометрические данные для Единой биометрической системы – это прийти с паспортом в отделение банка, который подключен к системе и пройти процедуру в специальном кабинете.

Одновременно рекомендуется использовать сложные и разные пароли, а также двухфакторную аутентификацию везде, где это возможно.

Также необходимо подозрительно относится к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься»), с темами про финансы, банки, в том числе со ссылками, особенно если они длинные или наоборот, использовались сервисы сокращения ссылок.

Нельзя переходить по ссылкам из письма, если они заменены на слова. Следует проверять ссылки, даже если письмо получено от коллеги или знакомого. Нужно помнить, что их аккаунты и личные кабинеты могли взломать. Также на фишинговом сайте часто есть орфографические ошибки и некорректно работающие элементы.

Что делать, если все же Вы стали жертвой:

- незамедлительно позвонить в банк (не по номеру из смс, а по номеру телефона, указанному на оборотной стороне банковской карты) и заблокировать счета и карты;

- сменить все пароли, которые вводились, особенно если они от онлайн-банков и «Госуслуг»;

- подать заявления в полицию, а также в Роскомнадзор о неправомерной обработке персональных и биометрических данных и хищении/попытке хищения денежных средств.

Главная защита от атак, связанных с биометрией, - это личная бдительность и понимание того, что Ваши уникальные данные нельзя передавать кому бы то ни было удаленно. Любая просьба это сделать – это верный признак мошенничества!

Следственный департамент МВД России