Babr24.com

Автор: Алиса Беглова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 5929 22.09.2020, 19:12
1

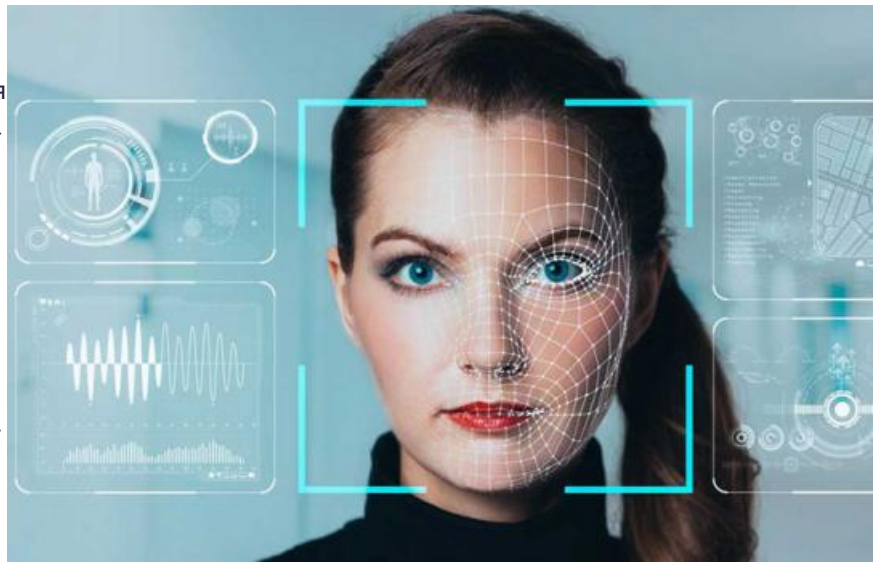
Банковские технологии — лазейка для мошенников?

Технологии в банковской сфере, с одной стороны, призваны повысить безопасность и защитить наши денежные средства от мошенников, но с другой — зачастую именно они и становятся той брешью в системе безопасности, через которую прорываются мошенники. Разбираемся, какие технологии действительно могут быть использованы злоумышленниками, а какие нет.

Биометрические данные

Кредитные учреждения активно собирают биометрические данные своих клиентов, чтобы сделать банковские сервисы более удобными в пользовании: например, удалённо открывать счета, переводить деньги с одной карты на другую. В числе таких биометрических данных — голос клиента, который банк предварительно записывает, чтобы потом, при обращении клиента за удалённой услугой, распознавать его.

Помимо записи голоса, банки также делают фото лица (специальная программа считывает уникальное для каждого человека расстояние от носа до глаз, от носа до губ), берут отпечатки пальцев, даже копируют рисунок вен ладони и сетчатку глаза.



Именно операции по голосу стали объектом паники среди населения. В социальных сетях можно увидеть паникёрские сообщения о том, что мошенники, записав ваш голос, могут от вашего имени осуществлять финансовые операции через колл-центр банка.

Однако представители банковской отрасли опровергают наличие такой лазейки для мошенников, поскольку необходимо не только разговаривать своим голосом, но также указать логин и пароль, полученные при регистрации в Единой биометрической системе (сюда банки передают биометрические данные, полученные от клиентов), а также назвать кодовое слово, а иногда также показать в камеру лицо. Так что одним голосом дело не ограничивается. Биометрическая идентификация клиента — многосоставный процесс.

Куда опаснее простейшие уловки мошенников, основанные на так называемой социальной инженерии — способах мошенничества, при которых злоумышленники с помощью психологических уловок заставляют жертву самостоятельно раскрыть все «явки и пароли».

Как показывает практика, почти в половине случаев мошенникам достаточно позвонить жертве, назвать её правильные имя, фамилию и отчество — и жертва проникается доверием к звонящему. Как правило, при таких звонках мошенники сообщают жертве легенду о блокировке карты или предлагают проверить данные.

Социальная инженерия разрастается. Новый способ украсть у вас деньги

Голосовое меню

А вот голосовое меню банков — куда более реальный механизм для мошенничества, притом открытый совсем недавно. В середине сентября Центробанк выявил следующую схему с использованием голосового меню в

колл-центре банков.

Злоумышленники обращались с подмененных номеров клиентов в систему интерактивного голосового меню банка. Следом запрашивали у системы сведения по остаткам денежных средств на картах клиентов, вводя для этого последние четыре цифры номеров этих банковских карт.

В дальнейшем мошенники, используя методы социальной инженерии, использовали полученные данные при осуществлении мошеннических звонков жертвам. То есть звонили жертвам, представляясь сотрудниками банков, и выуживали из них код-пароли, CVV-коды и прочие конфиденциальные данные.

Как следует из сообщения Центробанка, в результате утечки данных об остатке средств на счетах звонки от мошенников резко возросли у клиентов одного из банков, название которого не разглашается. ЦБ провёл расследование и выяснил, что данное кредитное учреждение не соблюдало рекомендации по противодействию мобильному мошенничеству и защите клиентов от несанкционированного доступа к их данным через систему интерактивного голосового меню.

Ранее на SmartBabr:

Главные киберугрозы-2020: фишинг, шпионы, трояны и бэкдоры

Автор: Алиса Беглова © SmartBabr

НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 5929 22.09.2020, 19:12 1

URL: https://babr24.com/?IDE=273496 Bytes: 4139 / 3668 Версия для печати

Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:
- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

Автор текста: **Алиса Беглова**, обозреватель.

На сайте опубликовано **257** текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта