Вся правда о безопасности банковских карт в телефоне

Apple Pay, Android Pay и Samsung Pay уже больше года работают в России, но до сих пор есть люди, которые боятся оплачивать покупки телефоном. Они переживают, что данные банковских карточек могут попасть к третьим лицам и привести к потерям на счетах. Павел Городницкий объяснил, как всё работает на самом деле.

Механика мобильных платежей элементарна: кассир называет цену, а покупатель

достаёт из кармана не карточку, а смартфон. Затем нужно либо снять отпечаток пальца, либо показать лицо фронтальной камере, либо просто ввести пароль, после чего гаджет одобрит покупку.

Потом — лёгкое касание терминала. Готово: деньги моментально списываются, а кассир выдаёт чек.

Почему это удобнее, чем платить картой?

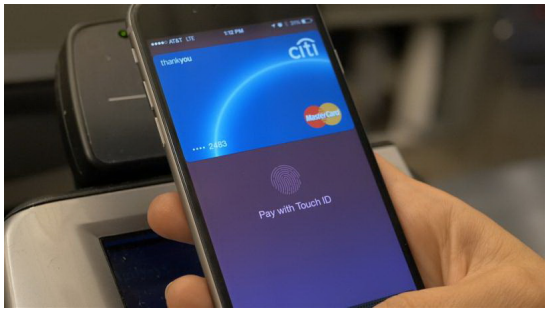
1. Не нужно ничего доставать из бумажника — можно просто извлечь телефон, который и так всегда под рукой.

2. Вводить пин-код приходится крайне редко, а вот при PayPass есть лимит беспарольных покупок (как правило, 1000 рублей). К тому же карты без PayPass тоже до сих пор живы: там пин-код требуют даже при "грандиозных" транзакциях на 10–15–20–150 рублей.

Сотни тысяч людей уже освоили и оценили Apple Pay, Android Pay и другие аналогичные

системы, пришедшие в Россию осенью 2016 года. Однако есть и те, кто уверен, что данные карточки могут попасть или к производителю смартфона, или к оператору, или вообще к хакерам, которые моментально опустошат счёт.

Пора рассказать, почему эти фобии беспочвенны. Логичнее всего пояснить схему на примере Apple Pay — тем более остальные сервисы функционируют по той же схеме.



Во-первых, Apple просто сотрудничает с банками, которые и настраивают процедуру обмена данными. Далеко не каждую карту можно внести в Apple Pay — всё зависит именно от банков, а не от условного Тима Кука. У компании из Купертино вообще нет контроля за обработкой транзакции. Представители Apple лишь договариваются, что генерируемые ими токены будут приниматься банком как валидное подтверждение оплаты. Токены в этом контексте — одноразовые пакеты, которые создаются на NFC-чипе и содержат информацию о транзакции (время, сумма, зашифрованные ключи).

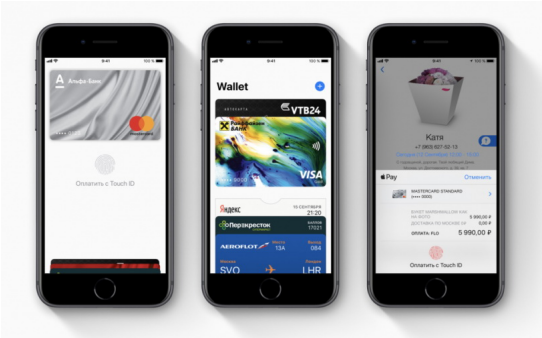
Во-вторых, единственный, кто получает данные карты при первом запуске Apple Pay, как раз выпустивший карту банк, который подтверждает её при стартовой настройке.

В-третьих, номер карты используется только один раз (первый, ещё при настройке), а затем не хранится вообще нигде. На отдельный чип (Secure Element в NFC-чипе, если быть точнее) в зашифрованном виде записывается специально сгенерированный номер счёта устройства (Device Account Number), который, даже если его уведут и расшифруют злоумышленники (что абсолютно нереалистично), не может использоваться совершенно ни для чего. Деньги с его помощью не украсть.

В-четвёртых, во время оплаты на терминал отправляются не данные карточки, а сгенерированный токен, который ещё должен быть подтверждён со стороны банка. Опять же: информацию о карточке в этот момент не получает вообще никто — к ней нет доступа в том числе у Apple. Кстати, на стороне банков действуют довольно продвинутые системы по распознаванию подозрительных транзакций, которые будут блокировать списание средств, если что-то пойдёт не так.

И **пятый пункт** для тех, кто ещё сомневается. Всё то же самое, что описано выше, происходит и при оплате через PayPass, но там токен генерируется чипом внутри карточки, а не смартфона.

Здесь же всё происходит на изолированном чипе внутри устройства, а генерация токена возможна только при подтверждении биометрическим сенсором или паролем.



PayPass даже уступает Apple Pay по уровню безопасности: мошенник может украсть карту и оплачивать ей покупки, не нарушая лимит (то есть не выходя за рамки 1000 рублей, если говорить о России). С телефоном так сделать не получится, если, конечно, жертва сама не разболтает пароль для оплаты.

Алгоритмы Samsung Pay и Android Pay такие же: передаётся исключительно токен, а не данные карточек. Правда, Samsung Pay ещё умеет оплачивать при помощи MST (Magnetic Secure Transmission), где поддерживаются даже устаревшие терминалы без NFC.

Такой способ считается чуть менее безопасным: в 2015 году компания LoopPay (её Samsung купила для создания платёжной системы) оказалась уязвима к атаке, которая позволяла перехватывать магнитный сигнал. Samsung Pay к тому моменту использовал токенизацию номеров
и защитный пакет KNOX и не был уязвим, но про теоретические уязвимости MST говорят и сейчас.

Поэтому, если вам нужна полнейшая безопасность, лучше довериться NFC-системам: они как минимум не менее надёжны, чем у классических бесконтактных карт. А по факту — даже надёжнее за счёт биометрических датчиков.

Источник

Тэги: на , они , что , могут , попасть , боятся , данные , покупки , банковских , карто чек , оплачивать , телефоном , переживают , лицам