

Будьте бдительны: деньги с карт научились воровать уже "по воздуху"

22 Января 2016, 15:31 | В России



В России появился новый вид мошенничества - кража денег с карт россиян, оснащенных технологиями бесконтактной оплаты товаров (карта прикладывается к PoS-терминалу, сумма покупки списывается с «пластика»), сообщает деловая газета «Золотой Рог».

По данным компании Zecurion, мошенники увели с карт россиян с помощью своих самодельных терминалов (RFID-ридеров) 2 млн рублей в 2015 году. Опрошенные компании, специализирующиеся на IT-безопасности, отметили, что мошенники научились воровать с карт с помощью смартфонов, оснащенных чипами NFC (NFC - разновидность RFID), пишут «Известия».

Технологии бесконтактной оплаты товаров разработаны американскими платежными системами Visa (PayWave) и Mastercard (PayPass) для ускорения и упрощения безналичной оплаты покупок. Карты с технологией PayPass выпускает 43 крупных российских банка, карты с PayWave - 16. Технологии PayPass и PayWave применяются на картах с чипом и магнитной полосой. При расчетах такой картой не нужно вводить PIN-код, а также ставить подпись на чеке, если сумма покупки небольшая (до 1 тыс. рублей). По оценкам Zecurion, карты с бесконтактной технологией оплаты есть у 2 млн россиян. Заявлено, что в России больше 30 тыс. точек приема PayPass: предприятия транспорта, торговли, сферы услуг.

Visa и Mastercard на своих сайтах, посвященных PayPass и PayWave, предусмотрели правила безопасности, но они не отличаются от тех, что выработаны для классических банковских карт (PIN-код должен быть неочевидным; его не следует писать на обратной стороне «пластика»; карта всегда должна быть в поле зрения, а телефоны для связи с банком - под рукой). PayPass и PayWave начали распространять в России в 2008 году, но до сих пор широкого распространения не получили: небольшое количество банков, эмитирующих такие карты, объясняется сложностью и дороговизной этой технологии, да и сама карта стоит дороже обычных на 50–100% (в зависимости от дизайна и типа карты).

Суть схемы похожа на перехват сигналов электрозамков угонщиками автомобилей. Как сообщили в Zecurion, средства с карт PayPass и PayWave списываются мошенниками с помощью самодельных считывателей, способных сканировать банковские карты с чипами RFID (см. фото). По большому счету это аналоги легальных бесконтактных PoS-терминалов: RFID-ридеров, посылающие электромагнитные сигналы.

- Хакерский ридер очень похож на легальное устройство, но он отличается более продвинутой функциональностью, - рассказал «Известиям» руководитель аналитического центра Zecurion Владимир Ульянов. - Рлоумышленнику достаточно приблизить на 5–20 см такое устройство к карте с чипом RFID, как вся необходимая информация будет считана.

В переполненном транспорте, на рынке, в магазине сделать это нетрудно. Человек может даже не заметить «воровства». Полученные данные мошенники записывают/передают на карты-клоны - для дальнейших операций (влекут хищения средств с подлинных банковских карт).

Стоимость легального считывателя для PayPass и PayWave - от 20 тыс. рублей. Но надо понимать, что хакерам для считывателя нужно немного, а компоненты не очень сложно заказать. Стоимость RFID-ридеров, которыми пользуются хакеры для воровства денег с банковских карт россиян, составляет \$100, - их хакеры изготавливают самостоятельно. Самый примитивный считыватель состоит из специального контроллера, антенны для приема сигнала и интерфейса для подключения к компьютеру и программного обеспечения на самом компьютере.

Как указывает замдиректора департамента аудита защищенности компании Digital Security Глеб Чербов, мошенникам достаточно бесконтактно получить номер карты и дату окончания срока ее обслуживания.

- Этих данных уже достаточно для проведения транзакций через подставные интернет-площадки или изготовления дубликата магнитной полосы карты, также достаточно для списания средств, - поясняет Чербов. - Из доступной «по воздуху» информации для злоумышленников также представляет интерес и история операций по карте, включающая в себя точные суммы и даты списаний. Располагая этими данными, несложно составить примерный профиль владельца и предположить текущий остаток по счету. У мошенников есть и более дешевые способы кражи данных с бесконтактных карт - обычный смартфон с поддержкой NFC. Им можно с расстояния в несколько сантиметров воровать данные банковских клиентов.

Но Чербов успокаивает, что защититься от мошеннической атаки не так сложно.

- Существуют кошельки, которые защищают карту от считывания (RFID blocking wallet), появились карты, которые кладутся в кошельки рядом с собственными - по цене около 500 рублей, - говорит Чербов. - Также пользователям новых карт можно посоветовать придерживаться давно известных рекомендаций относительно того, чтобы быть внимательными с SMS-информированием и соблюдать другие известные правила при проведении транзакций.

По словам замруководителя блока операционного и IT-сопровождения Бинбанка Игоря Новожилова, бесконтактное мошенничество пришло из Европы.

- Сложно предсказать потенциальный объем хищений, но с ним однозначно можно бороться, - уверен Новожилов. - Считывающее устройство должно быть поднесено практически вплотную к карте. Эта особенность уже обеспечивает определенный уровень защиты. Сложно представить, как кто-то допустит, чтобы по его карманам водили сканером. А если в кошельке две и более бесконтактных карты, то это только усложняет задачу считывания. Также можно менять порог суммы оплаты для ввода PIN-кода. Сама технология разрабатывалась для быстрых покупок на маленькие суммы, например оплата городского транспорта, прессы в ларьке и т.п.