## Приложение

## **Пять основных способов, при помощи которых мошенники**

## **опустошают карты граждан**

Недавно подписан закон, который ужесточает уголовную ответственность за хищение средств с банковских счетов или электронных денежных средств. За кражу средств закон устанавливает штраф в размере до 500 тысяч рублей или либо лишение свободы на срок до шести лет. Возможно, это остановит мошенников, но на сегодняшний момент кибератаки, вымогательство и шантаж с помощью компьютерных вирусов стали одной из главных угроз «цифровой» современности. Так, кражи денег с платежных карт за последний год сократились, но мошенники стали изобретательнее. Мы изучили пять основных способов, при помощи которых мошенники опустошают карты граждан. Как уберечь свои финансы от аферистов – комментирует Отделение по Владимирской области ГУ Банка России по Центральному федеральному округу.

1. **Выдал всё сам**

Нередко мошенники для кражи денег с карты пользуются психологическими приемами для управления действиями человека. Они изображают покупателей щенков, автомобилей, земельных участков, гаражей и т.д. на сайтах бесплатных объявлений или в социальных сетях. Общее у таких "покупателей" одно: они находятся где-то далеко, но для того, чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.

"Покупатель" просит продавца сообщить ему данные карты (код CVV2/ CVC2, срок действия, ФИО владельца), чтобы зачислить на нее деньги. Если доверчивый продавец сообщает эту информацию, с его карты начинают списываться деньги за оплату товаров и услуг, осуществляться переводы на другие счета и пр. В некоторых случаях злоумышленник пытается узнать код из смс, который приходит на мобильный телефон. Это значит, что мошенники уже сумели узнать данные карты и не хватает только кода подтверждения транзакции. Получив его, преступники похищают денежные средства.

Мошенники стали вовлекать даже детей. Путем случайных звонков, попадая на ребенка, ему говорят, что он выиграл крупный приз, и просят продиктовать номер банковской карты родителей и CV-код с обратной стороны. Но им при этом ничего не говорить. Мол, сюрприз будет. Также в интернете появились целые схемы, рассчитанные именно на детей, особенно, в мобильных играх и приложениях. Ребятам предлагают обменять их реальные деньги (например, на мобильном счете) на какие-то виртуальные знаки. Или без их ведома подключают к какой-нибудь платной подписке. Все больше платежей уходит на подобные подписки. А потом родители не понимают, куда у их детей исчезают деньги.

«В этом случае защитить владельца карты может простая осторожность. Не сообщайте данные карты, персональные данные и коды, присланные в смс, посторонним лицам. Не давайте никому доступ к вашей карте через онлайн-банкинг. В любых подозрительных ситуациях нужно звонить в банк, выдавший карту, по номеру, указанному на ее оборотной стороне», - рекомендует Надежда Калашникова, управляющий Отделением по Владимирской области ГУ Банка России по ЦФО.

1. **Кражи через банкоматы и POS-терминалы**

Чаще всего для кражи данных банковских карт злоумышленники атакуют POS-терминалы (аппараты для оплаты услуг). Эти терминалы обычно расположены в магазинах или аптеках и по сути представляют собой обычные компьютеры, доступ к которым можно получить через сеть WI-FI. Также злоумышленники крепят на банкоматы накладки-скиммеры, считывающие данные банковских карт.

Банковское сообщество ожидает активизациию кибермошенников перед Чемпионатом мира по футболу. Чемпионат стартует 14 июня и продлится месяц, соревнования будут сопровождаться массовым наплывом туристов и, соответственно, значительной нагрузкой на платежные терминалы и пункты обслуживания.

Банк России рекомендует гражданам не передавать свои карты посторонним, выбирать банкоматы в безопасных местах, не использовать устройства, которые запрашивают пин-код карты для входа в помещение и не вводить пароль при посторонних.

1. **Дубликат карты**

Деньги с банковской карты могут похитить даже там, где вы никак этого не ожидаете. Кассир, официант, заправщик, работник банка или любой другой сотрудник, которому гражданин передал платежную карту для расчета, может сфотографировать, переписать ее данные или просто запомнить их, чтобы потом изготовить дубликат карты. Сделать это можно незаметно. Заранее включается записывающее устройство (это может быть и обычная камера видеонаблюдения), на записи с которого карта видна с обеих сторон. В этом случае мошенникам остается лишь отмотать запись на нужное время и переписать данные карты.

Чтобы этого не случилось, не стоит передавать карту посторонним, рассчитываясь за покупку или предоставление услуг. Обратите внимание на поведение сотрудника, совершающего операцию. Если он фотографирует вашу карту на мобильный телефон под видом набора номера или смс, следует прервать операцию, потребовать возврата карты. И лучше всего обратиться в банк, выдавший карту, с заявлением о ее перевыпуске: ведь вы не знаете, какие данные он успел заснять.

1. **Двойная оплата.**

Представьте, что вы оплачиваете покупку в супермаркете. Передаете карту оператору, тот проводит ее через считывающее устройство.

Вы, если нужно, вводите ПИН-код. И тут кассир сообщает, что произошла ошибка, и оплата не прошла. Все повторяется сначала, и транзакция выполняется успешно. А спустя какое-то время вы обнаруживаете, что деньги за покупку были списаны дважды.

Удивительно, но даже те, у кого подключена услуга смс-информирования о совершенных операциях, не всегда сразу замечают исчезновение денег, думая, что вторая смс о списании средств - ошибка или дубль, так как суммы совпадают. Такие транзакции легко опротестовать и вернуть свои деньги. Но виновных сложно привлечь к ответственности, так как все можно списать на сбой в системе или ошибку оператора.

Честный кассир, если терминал оплаты действительно выдал отказ в проведении операции, всегда распечатает и выдаст покупателю чек, свидетельствующий, что оплата не прошла.

Подключите опцию смс-оповещений по операциям карты. Если первая транзакция совершена успешно, владелец карты тут же получит соответствующее смс-сообщение и сможет обосновать свой отказ от повторной транзакции, продемонстрировав его кассиру. Если вам поступило два сообщения о списании одной и той же суммы, позвоните в банк и проверьте, действительно ли произошло двойное снятие средств со счета.

1. **Бесконтактный грабеж**

Многие платежные системы разработали технологии бесконтактной оплаты для ускорения и упрощения безналичной оплаты покупок. Терминалами бесконтактных платежей чаще всего бывают оснащены торговые автоматы, платные автодороги, турникеты, автозаправки, супермаркеты и кафе. При расчетах такой картой не нужно вводить ПИН-код, а также ставить подпись на чеке, если сумма не превышает 1000 рублей. Специальный POS-терминал на расстоянии считывает информацию с карточки и звуковым либо визуальным сигналом дает понять, что необходимая сумма с нее списана.

В Россию эта технология пришла в 2008 году, и мошенники довольно быстро научились с ней работать. Злоумышленнику достаточно приблизить считыватель к карте на расстояние 5-20 сантиметров, чтобы списать деньги. В переполненном общественном транспорте, на рынке, в магазине злоумышленник прислоняет бесконтактный считыватель к карманам одежды, стенкам сумок и крадет деньги с карт у ничего не подозревающих владельцев. Полученную информацию мошенники могут записывать на карты клоны для хищения средств с настоящих банковских карт.

«Если вы пользуетесь бесконтактной системой оплаты, помните, что в качестве подтверждения списания суммы более 1000 рублей запрашивается PIN-код, а не подпись чека. Если вы не планируете оплачивать бесконтактным способом покупки на сумму более 1000 рублей, лучше всего установить индивидуальный расходный лимит по карте и ограничить количество возможных транзакций,» - предупреждает управляющий Отделением Владимир Надежда Калашникова.