Профилактика преступных посягательств в сфере использования информационно-телекоммуникационных технологий

Платежные карты, являясь удобным способом доступа к деньгам, оказываются объектом особого внимания злоумышленников, придумывающих все новые способы похищения этих денег.

Банки и платежные системы постоянно работают над повышением уровня безопасности платежей, производимых с помощью банковских карт. Между тем мошенники тоже становятся все более изобретательными и технически оснащенными.

**Чтобы обезопасить карты от посягательств**, владельцам "пластика" нужно знать основные правила безопасности и следовать им.

**Защита карты при онлайн-платежах.**

Наиболее распространенным является мошенничество с банковскими картами в Интернете, ведь именно ими сегодня расплачивается огромное количество покупателей в виртуальных магазинах. Часто мошеннику даже не нужна сама карта - достаточно информации о ней (номер карты, код CVV2/CVC2, СМС-пароль, подтверждающий данные и операцию по карте).

Чтобы уберечь от мошенников данные пластиковой карты при оплате товаров и услуг онлайн, следует соблюдать следующие меры безопасности.

Совершайте оплату покупок только на сайтах известных магазинов и компаний.

Для оплаты покупок через Интернет используйте отдельную банковскую карту, а не ту, на которой хранится основной объем ваших средств.

Переводите на карту для онлайн-платежей столько денег, сколько вы планируете потратить на покупки.

Следите за своевременным обновлением антивирусного программного обеспечения на устройствах, с помощью которых осуществляется оплата в Интернете.

Ограничьте возможность использования своей основной банковской карты за пределами региона вашего фактического местонахождения.

**Защита карты при использовании банкоматов и терминалов.**

При использовании банкоматов и терминалов очень важно не дать третьим лицам узнать ПИН-код и получить доступ к деньгам. Для этого нужно соблюдать следующие рекомендации.

Никогда не вводите ПИН-код на устройствах, не предназначенных для оплаты и снятия наличных.

При вводе ПИН-кода всегда прикрывайте клавиатуру рукой, чтобы его не могли подсмотреть находящиеся рядом люди или записать установленные злоумышленниками скрытые камеры.

Получив наличные в банкомате, не забывайте забрать платежную карту из картоприемника, а если все-таки забыли, незамедлительно заблокируйте ее.

Для проведения платежных операций через банкомат или терминал старайтесь не прибегать к помощи посторонних лиц, которые могут выдавать себя за работников банка.

Если денежные средства не были выданы банкоматом, но вы получили СМС-сообщение об их списании, заберите карту из картоприемника и незамедлительно обратитесь в ваш банк.

По возможности избегайте банкоматов, размещенных в местах массового скопления людей, особенно если снимаете крупные суммы денег. Старайтесь пользоваться банкоматами в отделениях банка или внутри зданий организаций и учреждений.

Установите суточный лимит на снятие наличных в банкоматах.

При использовании банкомата обратите внимание, не установлены ли на него посторонние устройства. Установка на банкомат высокотехнологичного устройства под названием "скиммер" - довольно распространенный способ кражи данных карты. Устройство считывает информацию с магнитной ленты и чипа карты, чтобы затем можно было ее продублировать. Если вам кажется, что отдельные детали банкомата выглядят подозрительно (их вид отличается от привычного) либо имеются какие-то дополнительные детали, не пользуйтесь таким банкоматом и сразу же сообщите о своих подозрениях в банк.

**Защита карты в общественных местах.**

В местах большого скопления людей (в переполненном общественном транспорте, на рынках, в магазинах) злоумышленник может не только украсть карту, но и приложить бесконтактный считыватель или POS-терминал к карманам одежды, стенкам сумок и снять деньги с карты, поддерживающей бесконтактную оплату, у ничего не подозревающей жертвы. Если вы пользуетесь картой с технологией бесконтактной оплаты (PayWave, PayPass или "Мир-бесконтакт"), следите, чтобы она не была легкодоступна.

**Защита от методов психологического воздействия.**

Многие схемы мошенничества, связанные с банковскими картами, основаны на технологии социальной инженерии. Они предполагают вытягивание из клиента конфиденциальной информации с использованием различных каналов коммуникаций (например, просят сообщить по телефону реквизиты банковской карты, одноразовые пароли) либо убеждение в совершении тех или иных действий под различными предлогами (например, представившись сотрудниками банка, просят подойти к банкомату и последовать инструкциям). Чтобы не стать жертвой мошенников (как онлайн, так и офлайн), рекомендуется следующее.

Никому не сообщайте ПИН-код и код CVV2/CVC2 своей банковской карты.

Никогда не давайте посторонним лицам данные карты, персональные данные и коды, присланные в СМС-сообщениях.

Не переводите и не зачисляйте деньги в ответ на просьбы, поступающие с неизвестных номеров.

Если вы получили сообщение якобы от близкого родственника с просьбой положить на счет деньги, перезвоните родственнику, используя номер из своей записной книжки, уточнив, соответствует ли действительности полученная вами ранее информация.

Не набирайте на мобильном устройстве цифровые команды, назначение которых вам неизвестно.

**Как избежать неприятностей, связанных с потерей или кражей карты.**

Беречь платежную карту нужно так же, как берегут наличные деньги: от механических повреждений, от воздействия влаги. Держите карту вдали от электроприборов и других электромагнитных излучателей.

По договору с банком ответственность за сохранность карты лежит на ее владельце. Поэтому не передавайте ее третьим лицам, даже членам семьи, и не сообщайте никому ее ПИН-код. Если вы не можете запомнить ПИН-код, его ни в коем случае нельзя писать на карте - держите запись в недоступном для посторонних месте.

Обязательно распишитесь на оборотной стороне вашей карты. Перепишите и храните в недоступном месте реквизиты карты и телефон кредитной организации, размещенный на карте: они пригодятся вам в случае потери или кражи банковской карты, чтобы своевременно ее заблокировать.

Резонно устанавливать личные суточные или месячные лимиты, ограничения регионов ее использования. Эффективной мерой контроля является услуга СМС-информирования, при которой контрольное СМС-уведомление об исполнении или отклонении каждой операции по банковской карте приходит на мобильный телефон владельца. Постоянно контролируйте расходы денежных средств на счете карты.

Если карта все же потеряна или украдена, следует срочно связаться со службой поддержки клиентов вашего банка по телефону или отправить сообщение по мобильному банку (если такая услуга подключена), проинформировать о сложившейся ситуации, попросить заблокировать карту и сделать заявку на ее перевыпуск. Для более оперативной связи с банком рекомендуем всегда иметь при себе телефон службы клиентской поддержки, а также сохраненное СМС-сообщение с текстом-командой для блокирования карты. Обязательно в кратчайшие сроки подтвердите свой звонок письменным заявлением в офисе банка.

Если вы пользуетесь услугой "Мобильный банк", не забывайте своевременно уведомлять кредитную организацию о смене номера телефона мобильной связи. А в случае потери мобильного телефона нужно незамедлительно связаться с банком и заблокировать карту.

В случае если Вы все же стали жертвой мошенников, Вам необходимо обратиться с заявлением в дежурную часть ближайшего к вам отделения полиции, либо в прокуратуру.

Прокуратура Уйского района