«Осторожно, мошенники!» МО МВД России «Аркадакский» предупреждает!

Поскольку банковские карты прочно входят в нашу жизнь и ими, картами, пользуются практически все начиная от студентов и заканчивая пенсионерами, то естественно мошенники не могли остаться в стороне. Мошенники всеми возможными способами пытаются заполучить данные карты пользователя – начиная от номера карты и заканчивая пин-кодом. Банковское мошенничество один из наиболее распространённых способов изъятия денег в Интернет, мошенники «работают» с платёжными картами, с зарплатными картами, а так же с дебетовыми картами.

Мошенничество с использованием платёжных карт:

Мошенничество с пластиковыми картами происходит несколькими способами. Один из самых простых способов является рассылка фальшивых смс или звонок от имени банка. Схема очень простая, абоненту приходит смс вида – «(Bank). Заявка с карты 6000 р. Принята», «(Bank).Ваша карта заблокирована». В каждом таком смс содержится номер телефона злоумышленников, выдаваемый за номер службы поддержки банка. Абонент звонит на этот номер, где ему говорят, что карта заблокирована/произошла техническая ошибка и нужно выполнить несколько простых действий:
- Найти банкомат и выполнить действия, диктуемые фиктивным сотрудником банка. Как результат – пользователь лишается некой суммы на счету карты.
- Просят сообщить данные карты, в том числе пин-код. Впоследствии злоумышленники, зная все данные пользователя, просто переводят денежные средства с карты пользователя.

Запомните! Сотрудники банка никогда не требуют у клиентов выдачи личных данных и пин-код, и точно никогда не попросят Вас проводить какие-либо операции с банкоматом. Особенно популярно такое мошенничество с картами сбербанка, т.к. именно в сбербанке обслуживаются большинство государственных учреждений, а так же пенсионеры – самые незащищенные и доверчивые слои населения.

Если Вы получили SMS-сообщение из банка с уведомлением о приостановке обслуживания карты/списании средств или Вам позвонили, представившись сотрудником банка, и просят предоставить сведения о карте или другую личную информацию – ничего не предпринимайте, а позвоните в банк и уточните полученную информацию. Обязательно используйте только официальный номер службы поддержки Вашего банка.

Но, к сожалению, мошенничество с кредитными картами не ограничивается этим, в интернете очень часто злоумышленники подсовывают фальшивые сайты (фишинговые) (например «Ростелком»), где требуют ввод номера карты и csv кода. После того, как пользователь ввел данные – ловушка захлопнулась, и скорее всего в ближайшее время пользователь лишится денежных средств, хранившихся на карте.
И по-прежнему актуальным вопросом остается отношение самих граждан к электронным носителям информации. В первую очередь это касается пожилых граждан, которые в свой кошелек кладут и записку с пин-кодом банковской карты. Впоследствии где-нибудь оставляют, теряют свой кошелек. Нашедшему остается только воспользоваться такой удачей.

Граждане, будьте предельно внимательный и не оставляйте данные карты на сайтах в которых Вы не уверены и не носите с собой в одном месте с банковской картой записку с пин- кодом. Если Вам трудно запомнить пин-

код, постарайтесь хотя бы спрятать записку с ним в другом месте - в паспорте, в любом из карманов одежды либо оставить пин-код у родственников, которым Вы доверяете.

Участились случае почтовых мошенничеств.

Схема проста: создаются сайты-«однодневки», где указаны товары с «огромной» скидкой. Для заказа выбранного вами товара необходимо лишь имя и ваш абонентский номер. После ввода вашего абонентского номера вам поступает звонок, в ходе которого вам предлагают различные акции и бесплатную доставку. Все это направленно на увеличение среднего чека. Так же вас будут убеждать, что на товар действует гарантия и в случае несоответствия, товар можно отправить обратно. Все это направленно на увеличение среднего чека. Через несколько дней после оформления заказа, на ваш телефон приходит смс-уведомление с трэк-номером для отслеживания почтового отправления. Зачастую, отправки происходят от ООО «Пост-сервис» или же от частного лица. Когда отправление поступает в ваше почтовое отделение, опять же на ваш телефон приходит смс-уведомление типа: «Получите отправление в ближайшие 3 дня, и мы дадим вам скидку 50% на следующий заказ или пополним ваш баланс мобильного телефона». Все это направлено на максимальную скорость отъема денег. Мошенники пользуются тем, что на почте при получении отправления с наложенным платежом - данное отправление нельзя получить в руки и вскрыть, предварительно не оплатив, а оплатив – вы там обнаруживаете не соответствующий товар, который нельзя отправить обратно и вернуть свои денежные средства, таковы почтовые правила.