МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

Интернет - удобный способ получить доступ к любой информации, имеющейся в сети. Однако интернет может нести за собой опасность.

Реквизиты карты это информация, которую Вы можете увидеть (прочитать) на самом «пластике»:номер из 16 цифр, имя и фамилия владельца, срок действия и трехзначный код безопасности на обратной стороне.

По правилам платёжных систем реквизиты категорически запрещено сообщать посторонним. Зная реквизиты карты, злоумышленник может

-совершать любые платежи, начиная с оплаты товаров и заканчивая мгновенными денежными переводами.

*Никогда не сообщайте своих личных данных непроверенным людям. Сотрудники банка никогда не будут у вас просить пароль для дocmyna к банковскому счету.*

Рассмотрим некоторые распространённые виды мошенничества в Интернете.

1. Вы можете получить СМС-сообщение или письмо, в котором, Вы якобы являетесь победителем в лотерее, либо Вы получили открытку или Вам предлагают скачать программу по ссылке.
2. Мошенники, якобы продающие товар или оказывающие услуги, зачастую размещают свои объявления на досках объявлений, например, ru. Они требуют предоплату на кошелек или номер телефона. В большинстве случаев это развод на деньги, необходимо игнорировать подобные предложения.
3. Мошенники зачастую могут использовать против Вас информацию, которую Вы разместили в сети интернет в открытом доступе:

* *Ваши фотографии,*
* *Ваш номер телефона ;’*
* *Ваш адрес.*

*Полученную информацию они могут использовать, в частности, для вымогательства у Вас денежные средств за нераспространение той или иной личной информации.*

1. В интернете могут встретиться различные подставные сайты, самый распространенный сайт требующий якобы уплату штрафа за якобы просмотр порнографических изображений в сети Интернет.

*Baжнo! Помните, что штрафа за подобную деятельность не предусмотрено, если на Вас налагается штраф компетентным органов, он придет Вам по почте заказным письмом.*

1. Зачастую мошенники предлагают в социальных сетях якобы возможность быстрого и легального заработка больших сумм денег или легкого взятия кредита.
2. Также злоумышленники действуют, а именно взламывают аккаунт (социальной сети) и рассылают сообщения с просьбой о помощи якобы от имени его владельца. Чаще мошенники, представляясь друзьями, скидывают номер банковской карты и просят перечислить на нее деньги. В настоящее время пошли дальше - для большей убедительности присылают скриншоты "пластика" с именем и фамилией владельца
3. Наверное, многие белорусы знают площадку по продаже [kufar.by.](http://www.kufar.by/) Достаточно простой и удобный интерфейс, много посетителей, для продажи вещей.

Вот вам «маячки», которые помогут не попасть на удочку мошенников:

* Все очень просто и быстро (у вас сразу хотят купить товар, ничего не расспрашивая про него)
* Избегают общения голосом
* Звонят и пишут в мессенджерах зарубежных операторов
* Вам присылают какие-то ссылки
* Вам рассказывают про сервисы доставки, о которых вы не слышали
* Вам надо ввести данные своей карты, не только номер, но и 3-x значный код на обратной стороне

1. Вишинг: мошенники обзванивают клиентов, представляясь сотрудниками различных служб банков. Звонок поступает па мобильный телефон или в мессенджер (Viber, WhatsApp). Чтобы войти в доверие, злоумышленники могут обращаться по имени, назвать адрес или часть цифр номера карты. Получив информацию, мошенник списывает деньги со счетов. Кроме того, бывают случаи, когда таким образом склоняют к оформлению на свое имя кредита, после чего также выманивают сведения о банковской карте (номере договора) кредита и похищают денежные средства.

Виды:

А)отмена перевода/заявки на кредит.

Б) участие в спецоперации.

В) отмена заказа на покупку/доставку товара