* **Интернет продажи**

это дубликаты интернет страниц популярных брендов или специально созданные сайты с кричаще низкими ценами на товары или услуги, вы заказываете товар оплачиваете его на сто процентов указанным там способом и ждете когда его привезут.

**КАК СЕБЯ УБЕРЕЧЬ**

Делайте покупки только на официальных и проверенных сайтах, старайтесь не расплачиваться банковскими картами или заведите себе специальную банковскую карту, на которой будет только необходимая для покупки товара сумма. Читайте отзывы к выбранному Вам сайту, но не на нём а на форумах посвященным мошенникам (их множество).Обращайте внимание на заниженные в разы цены.

* **Продажи в соц сетях**

Вам от имени Ваших контактов или от других источников рекомендуют группы или лиц занимающихся продажами товаров и услуг, после этого Вы заказываете товар или услугу, производите оплату но в замен кроме расстройства ничего не получаете.

**КАК СЕБЯ УБЕРЕЧЬ**

Не делайте предоплат, читайте отзывы к выбранному Вам контакту или группе на форумах посвященным мошенникам (их множество).Обращайте внимание на заниженные в разы цены.

* **Блокировка компьютеров**

Распространенный в интернет среде **вирус** в различных модификациях, влияющий на работоспособность Вашего персонального компьютера, а именно не возможность его использования по назначению в связи с отсутствием доступа к системным функциям. Обычно блокировка компьютера сопровождается предупреждающими надписями вроде «Вы смотрели запрещенные фильмы или скачивали запрещенные программы» с требованием заплатить штраф, перечислив денежные средства на указанный счет, это так же может быть и другие тексты но смысл у них один, **вы должны заплатить штраф.**Указанные вирусы попадают в Ваш компьютер через электронную почту письма (из судов, банков) которые Вы не ждете и не могли бы получить, через не лицензионные игры и программы.

**КАК СЕБЯ УБЕРЕЧЬ**

Установите на устройство лицензированное антивирусное обеспечение (какое выбор за Вами) он обойдется дешевле потерянных денежных средств, не открывайте файлы, электронные сообщения поступившие от неизвестных источников, не скачивайте бесплатный коннект с подозрительных сайтов, не сохраняйте на устройстве пароли.



**ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!**

**ОСТЕРЕГАЙТЕсь УЛОВОК ПРеСТУПНИКОВ!**

**ОНИ ПОДГОТОВИЛИ ДЛЯ ВАС СЛЕДУЮЩИЕ ЛОВУШКИ!**

* **СКИММИНГ (чтение данных)**

Это хищение данных с магнитных лент банковских карт, обычно оборудование устанавливается на банковских терминалах (банкоматах) поверх считывающего устройства и клавиатуры и внешне выглядит как заводское, могут использоваться с миниатюрной видеокамерой закрепленной у монитора, этом при считывании данных вашей карты преступники получают доступ ко всем вашим персональным данным, включая пин-код, после чего изготавливают дубликат банковской карты и снимают с его помощью денежные средства, предпочитая при этом иностранные государства.

**КАК СЕБЯ УБЕРЕЧЬ**

При операциях с пластиковыми банковскими картами в терминалах самообслуживания (банкоматах), отдавайте предпочтение оборудованию, расположенному в банковских залах, так как они наиболее защищены от установки скиммингового оборудования. По возможности не пользуйтесь терминалами установленными в местах большого скопления людей (аэро и ж/д вокзалы, гипер и супер маркеты, уличные банкоматы)

* **ФИШИНГ (рыбалка)**

Преступник делает смс-рассылку сообщений с текстами «Ваша карта заблокирована (аннулирована), для разблокировки свяжитесь с банком по телефону +7\*\*\*\*». Обычно сообщения приходят с обыкновенных номеров операторов связи России, но могут быть направлены и с коротких трех четырехзначных номеров. При разговоре псевдо банковские работники сообщают Вам, что необходимо подойти к терминалу и следуя указаниями «оператора» ввести определенную комбинацию цифр.

Может случиться так, что Вас попросят продиктовать номер карты, номер обозначенный на обратной стороне карты под магнитной полосой, срок действия карты и пин-код,

**КАК СЕБЯ УБЕРЕЧЬ**

Не верьте ни кому кто бы к вам не обращался по телефону и от чьего бы лица он ни выступал, не верьте смс-сообщениям с указанием телефонных номеров не принадлежащих Вашему банку. В случае сомнения, позвоните по телефону указанному на обратной стороне **Вашей банковской карты** и послушайте совета специалиста или пройдите к ближайшему офису Вашего банка. Не сообщайте ни кому и ни при каких обстоятельствах пин-код и другие сведения о банковской карте. **Помните, чтопин-код не известен даже сотрудникам банка.**

* **МОБИЛЬНЫЙ ВИРУС**

Новинка от преступников для пользователей мобильных устройств работающих на платформе OCAndroid СМС-Троянец, это самый обыкновенный вирус попадающий в Ваше устройство через электронную почту, смс-сообщения или сообщения получаемые в социальных сетях- Trojan-Ramson.Win32.Cryaki.bo.

Его цель, завладеть Вашими персональными данными и в частности сведениями о привязке к Вашему телефонному номеру банковских карт после чего этот самый **вирус** без вашего участия переводит ваши денежные средства на нужные преступникам счета, при этом ни каких смс-оповещений об операциях Вам не поступает.

**КАК СЕБЯ УБЕРЕЧЬ**

Установите на мобильное устройство лицензированное антивирусное обеспечение (какое выбор за Вами) он обойдется дешевле потерянных денежных средств, не открывайте файлы, смс-сообщения поступившие от неизвестных источников, не скачивайте бесплатный коннект с подозрительных сайтов, не сохраняйте на мобильном устройстве пароли.