Ханты-Мансийская городская организация Общероссийской общественной организации «Всероссийское общество инвалидов»

ГРАНТ ГУБЕРНАТОРА ЮГРЫ

Выпуск №2

# «Использование сети интернет при совершении хищения денежных средств»

Фото автора Tima Miroshnichenko: Pexels

Только внимательное отношение к своим персональным данным и реквизитам банковских карт существенно снизит риск хищения ваших денежных средств с банковского счета

- Все преступления, совершаемые посредством современных компьютерных технологий и сети интернет можно разбить на несколько групп. Наиболее часто встречающиеся виды преступлений мы попробуем разобрать в серии аналогичных буклетов для предупреждения жителей округа о том, что нужно предпринимать, что-бы не стать жертвой преступников и избежать финансовых потерь.
- Помните, никому и ни при каких обстоятельствах не сообщайте данные вышей банковской карты: номер, дату действия, три цифры с оборота карты.  Этих данных преступникам достаточно для хищения денежных средств с вашей банковской карты.

# Обман через интернет: безопасная сделка на авито

**Как это происходит:** Вас заинтересовало сообщение на сайте «авито», и в ходе разговора продавец предлагает воспользоваться «безопасной сделкой авито». В ходе переписки преступник присылает вам ссылку на сайт, оформленный в стиле «авито-безопасная сделка», на данном сайте требуется ввести данные банковской карты для получения денежных средств.

**Что на самом деле:** Целью преступников является завладение данными вашей банковской карты. На самом деле вам присылают ссылку на сайт-обманку, который принадлежит преступникам. Как только вы вводите данные своей банковской карты, с нее начинают похищать денежные средства.

**Как поступать**: Ни при каких обстоятельствах не переходите по ссылкам, присылаемым вам другим покупателем или продавцом. Преступники в ходе разговора будут пытаться перевести диалог с официального сайта в вайбер или вацап, поскольку официальный сайт распознает ложные ссылки и блокирует такие сообщения. Необходимо сразу прекратить общение с таким человеком. Он не собирается вам что-либо продавать или покупать у вас. Его цель – ваша банковская карта.

# Обман через интернет: продажа через авито

**Как это происходит:** Вы выставили объявление о продаже товара, договорились с покупателем, он попросил отравить товар в другой город. В день выдачи товара вы не можете войти в свой аккаунт, а покупатель получает товар в пункте выдачи. Вам деньги не приходят.

**Что на самом деле:** Преступники, договорившись с вами о покупке товара и отправке его в другой город, через телефон/интернет меняют ваши данные на сайте авито, в том числе номер телефона и электронную почту. В момент прихода товара в их город преступники от вашего имени подтверждают возможность выдачи товара. Товар выдается преступникам, а деньги вам не поступают.

**Как поступать**: Если вы продаете товары через сайты аналогичные авито, то постоянно отслеживаете данные которые введены на сайте: номер телефона, емайл, контактные данные. Внимательно следите за приходящими смс и электронными сообщениями, в которых указывается о смене каких либо данных. В случае обнаружения подозрительной активности, незамедлительно уведомляйте об этом службу поддержки авито, блокируйте выдачи товара и отменяйте сделку. Это поможет избежать хищения вашего товара.

# Обман через интернет: покупка по предоплате

**Как это происходит:** Вы заказываете на сайте покупку, к примеру телефона, по очень привлекательной цене, оплачивайте его на сайте, а товар не приходит. Телефон поддержки не отвечает, сайт прекращает свою работу.

**Что на самом деле:** Преступники создают сайт-пустышку в виде интернет магазина, в котором размещают товары со скидкой 10-50% от рыночной цены. Вы производите покупку, перечисляете денежные средства, а товар вам не отправляют. Деньги перечислены на «левый» счет, фирма не существует или оформлена на подставное лицо. Более худший вариант, когда вы ввели данные своей банковской карты на таком сайте. Тогда вы лишаетесь не только денег за товар, но и всех денег со своего счета.

**Как поступать**: Не покупайте товары на малознакомых сайтах по предоплате. Оформляйте покупку с функцией «оплата курьеру, при получении». Не вводите данные своей карты на сторонних сайтах, избегайте дистанционной оплаты за поставляемые товары. Проще переплатить за услугу «оплата курьеру» чем пытаться найти преступников которые похитили ваши денежные средства.

# Обман через интернет: покупка снегохода

**Как это происходит:** На специализированном сайте известной фирмы-продавца Вы увидели спецтехнику по привлекательной цене. Отзывы на сайте положительные. Созвонились с менеджером, договорились о поставке, оплатили товар. На этом ваше общение с менеджером прекратилось. Товара нет, телефон не отвечает, отрицательный отзыв с сайта удален.

**Что на самом деле:** Преступники, пользуясь вашей невнимательностью, создали сайт-клон официального продавца, адрес которого отличается на одну букву. К примеру, если официальный сайт производителя написан так «http://irbismotors.ru/», то сайт подделка зарегистрирован на таком домене: «https://irbis-moto.nethouse.ru/». Все отрицательные отзывы удаляются. Обычно, такие сайты существуют непродолжительное время, и, как только, обманутых клиентов стало много, сайт перестает функционировать а все контактные телефоны не отвечают. Перечисленные вами деньги похищены, товар вам никто никогда не отправит.

**Как поступать**: Не покупайте товары на малознакомых сайтах. Не верьте отзывам в интернете, которые пишут на том-же сайте, на котором вы собрались покупать. Администрация сайта может удалять плохие комментарии. Помните, что скупой платит дважды. Лучше приехать и забрать товар самостоятельно, чем рисковать с покупкой через интернет «кота в мешке».

# Обман через интернет: вы выиграли приз третей категории 1 120 000 руб.

**Как это происходит:** Вам через вайбер или вацап поступает сообщение, о том, что ваша транзакция по карте visa/masterCard вошла в число призовых. За вами закреплен приз третей категории 1 120 000 рублей. Для получения выигрыша свяжитесь с призовым отделом или перейдите на сайт компании.

**Что на самом деле:** Такое сообщение поступило представителям нашей команды, которая реализует данный проект, и мы решили проверить, что будет происходить далее. Мы использовали абсолютно новый номер. На сайте, который был указан в сообщении, нами пройдена регистрация под выдуманным именем. И оказалось, что наш номер, с выдуманным именем выиграл тоже 1 120 000 рублей. С нами связался представитель компании, и по телефону начал очень много говорить, убеждать в том, что нам круто повезло, для получения денежных средств нужно только заплатить 13% налога, а точнее только 1/10 от 13%, и то эти деньги нужно забросить на свой номер телефона. В ходе разговора менеджер много говорил, тараторил, не выпускал из внимания. Просил подойти к банкомату для пополнения телефона. Сообщил что сейчас придёт специальный код для регистрации в системе. На самом деле, пришло смс с кодом регистрации в одной из платежных систем. Преступник просил назвать этот код, и догадавшись, что мы ему не верим, и код называть не будем прервал разговор.

**Как поступать**: Бесплатный сыр только в мышеловке. Это обман чистой воды. Сайт сделан красиво, но при внимательном рассмотрении на нем много грамматических ошибок, к примеру «Тркнажер Ketler». На сайте работает целая группа мошенников: одни общаются через сайт, другие работают по телефону. Самым правильным будет при получении такого сообщения, это его удалить, никому не пересылать, не переходить по указанным ссылкам и никогда не звонить по указанным телефонам. Со своей стороны м направили обращение в управление К МВД и РУ-Центр для блокировки указанного сайта.

# Обман через интернет: ИТОГИ

Помните, никогда, никто ни при каких обстоятельствах не будет раздаривать призы и подарки, возвращать вам компенсации или выплачивать крупные денежные призы. Все это обман, рассчитанный на вашу невнимательность, доверчивость. Не позволяйте обстоятельств взять верх над вами. Трижды перепроверяйте всю информацию в интернете, и, если заметили что либо подозрительное – откажитесь от сотрудничества с этими людьми.

Запомните:

**До тех пор пока вы сами не сообщите на сайте или в интернете коды доступа к вашим личным кабинетам или банковским картам, с них практически невозможно похитить денежные средства.**

Если вы стали жертвой мошеннических действий, незамедлительно обратитесь в полицию с заявлением о совершенном в отношении Вас преступлении.