Мошенничество в интернете

Сделал: Балуев Валера

Как избежать мошенничество в интернете?

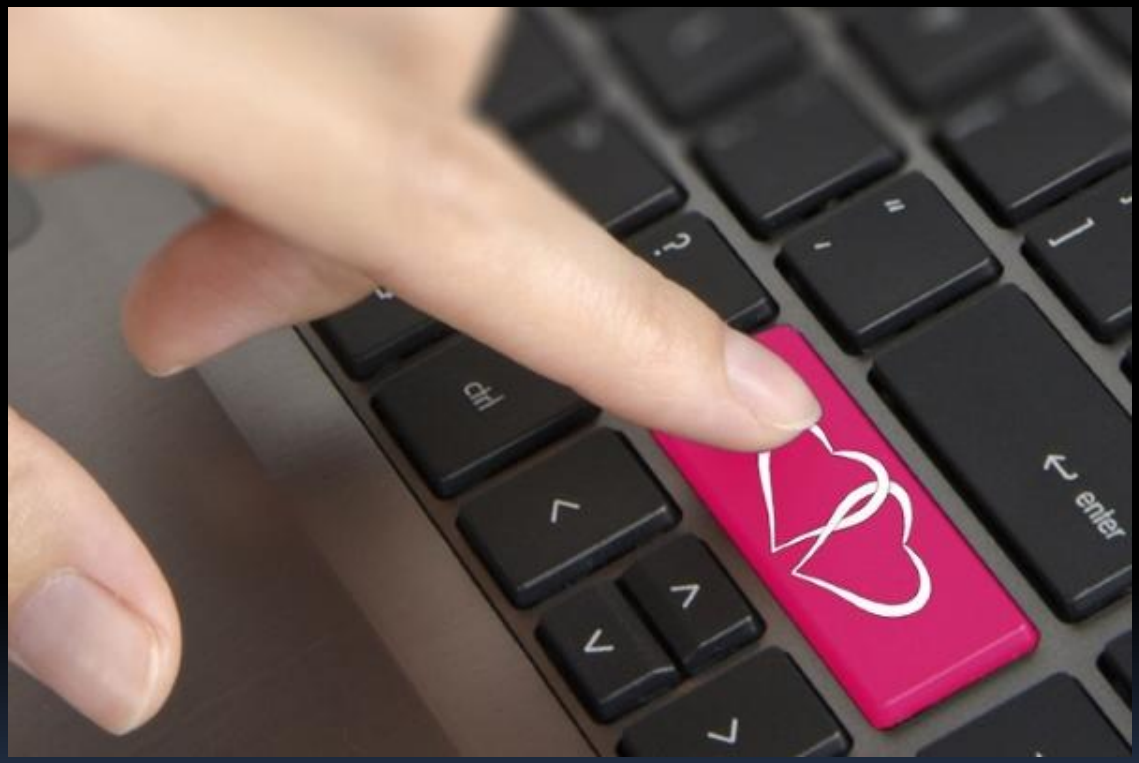
- Первая — общие **нормы безопасного поведения в интернете**. Их нужно соблюдать всегда, при любых условиях или действиях, даже при обычном поисковом запросе через Гугл или Яндекс.
- **Не заходить на подозрительные сайты**. Если случайно открыли такой — сразу же закрывайте. Степень доверия любому ресурсу можно определить интуитивно, но советуем ознакомиться с признаками мошенничества. Мы постарались описать характерные черты сайта, который скорее всего используют для выманивания денег.
- **Не скачивать файлы сомнительного характера.** Лучше всего использовать официальные сайты программного обеспечения, если вы не хотите заразить свой компьютер вирусами.
- **Регулярно обновлять антивирус**. Об необходимости этого даже не нужно объяснять, чем лучше защищен ваш собственный компьютер, тем меньше шанс получить вредоносную программу.
- **Не выключать брандмауэр**. Некоторые сервисы, онлайн-игры и другие сайты для корректной работы просят вас отключать встроенную систему интернет-защиты (брандмауэр). Мы советуем этого не делать и избегать такие проекты.
- **Регистрировать e-mail на надежных сервисах**. К примеру, аккаунт Google считается очень защищенным, тогда как некоторые другие системы уже известны обилием «дыр» в защите.
- **Не читать спам и не открывать письма с прикрепленными файлами.** Из самого понятия спама понятно, что он не содержит осмысленной информации и его лучше регулярно удалять. Особое внимание письмам, которые содержат вложенные файлы. Узнать их легко — обычно рядом с таким сообщением нарисована «скрепка». Если не уверенны, от кого оно пришло — ни в коем случае не открывайте.

Как в соцсетях отличить от мошенничества настоящую просьбу о помощи?

Посмотрите, указан ли город, в котором требуется помощь. Почти все объявления от мошенников пишутся без географической привязки. Это делается для того, чтобы каждый подумал, что это случилось в его населенном пункте. Так что отсутствие города — первый признак обмана. Обратите внимание на наличие деталей в объявлении. Зачастую их просто нет. Непонятно, к кому обращаться, остается загадкой и возраст щенков, и сколько из них мальчиков и девочек. Если речь идет о больном ребенке, то не указываются диагноз, больница, в которой он лежит, адреса отделений переливания крови, график их работы и другие очевидные вещи.

Как разводят на сайтах знакомств и как не стать жертвой мошенничества?

На сайтах знакомств мошенники способны действовать по-разному. У них имеется несколько отлаженных схем, зная которые можно распознать преступника и обезопасить себя. Чаще жертвами обманщиков становятся доверчивые и сентиментальные женщины любого возраста и определенного социального положения.



Женщины любят щедрых.

- Этот способ похож на предыдущий, поскольку ориентирован на женскую доверчивость и любовь к подаркам. Пользуются таким способом обмана мошенники, выдающие себя за иностранцев. Схема такова: после продолжительного общения мужчина говорит женщине, что хочет выслать ей подарок в виде дорогой вещи – Айфона, ювелирного украшения или брендовой сумочки. Для этого ему только необходимо узнать номер телефона женщины для заполнения контактов получателя на почте. По прошествии некоторого времени на телефон женщине приходит СМС от курьерской службы, в котором требуется перечислить по указанным реквизитам средства за оплату доставки посылки из-за рубежа. В переписке с щедрым поклонником выясняется, что у него то ли не было возможности оплатить доставку (например, курьерский сайт якобы принимает только оплату Яндекс-деньгами), то ли он просто забыл это сделать, но обещает возместить все траты со дня на день. Доверчивая дама перечисляет необходимую сумму (обычно около 50 долларов) и ожидает свой подарок. По закону жанра ни посылки, ни денег, ни воздыхателя женщина в итоге не получает. После получения денег мошенник удаляет анкету с сайта знакомств, а все его данные, которые женщина могла запомнить, оказываются недействительными и отыскать его будет проблематично. А сайт якобы курьерской службы оказывается фейковой страничкой.

Опасные интернет-магазины – с первого взгляда

- Распознать ложный ресурс можно также по отсутствию:
- подробного описания товаров;
- реквизитов владельца, контактов, адресов;
- данных юридического лица;
- ссылок на поставщиков, производителей;
- информации о возврате, точного описания гарантий;
- различных способов для оплаты (чаще всего предложены электронные кошельки).
- На таком сайте:
- есть много информации о безопасности и конфиденциальности;
- указаны 1-2 номера, чаще — мобильные;
- в адресной строке — незащищенное соединение (http вместо https).

Способы мошенничество

- Разводы интернет-магазинов:
- «Зеркала». Копируют брендовые магазины типа Lamoda или OZON, наживаются на авторитете компании. Иногда покупателям удается забрать товар, но приходит дешевая подделка, а не обещанный бренд.
- Игнорирование клиента после оплаты товара. Деньги перечислены, продавец не отвечает, техническая поддержка молчит, покупки нет.
- Некомплект, то есть не хватает запчастей, элементов одежды и т.д.
- Несоответствие описанию. Мошенники присылают товар другого цвета, формы, качества.
- Заказанный продукт пришел сломанным, просроченным, бракованным.
- Продавец заставляет доплатить. В процессе оформления заказа возникает необходимость доплатить за доставку. Или фактическая стоимость услуги оказывается выше той, что была обозначена на сайте.
- Отсылка к ненадлежащей работе почтовой службы. Якобы продавец отправил товар, а почта его потеряла. Аферист даже может предоставить трек для отслеживания, конечно же, липовый.
- Передача данных третьим лицам, хищение средств с карты или электронного кошелька.

Как вычислить лохотрон?

- Признаки, которые помогут распознать лохотрон:
- оплата заказа по номеру телефона или на электронный кошелек;
- в интернете нет отзывов, или большинство из них отрицательные;
- на свободных ресурсах нет информации о магазине;
- техническая поддержка не отвечает или форма обратной связи отсутствует;
- магазин работает по полной или частичной предоплате;
- доставка только почтой;
- возраст сервиса 2-3 месяца (это можно проверить через домен, не всегда истинный возраст совпадает с тем, что указан в информации на сайте).
- Если вы заметили хотя бы один из названных признаков, то стоит отказаться от покупки в этом магазине.

Как не попасть в руки мошенникам!

- **Персональная информация**
- При отправке личной информации о себе, в том числе на форумах, чатах, магазинах, и оставляя комментарии к статьям, будьте осторожны. Во многих случаях информация, которую Вы размещаете на сайтах, будет там находиться постоянно. Поэтому старайтесь не размещать на сайте информацию личного характера (номера телефонов, адрес, номер кредитной карты и пароли). Прежде чем разглашать личные данные о третьих лицах, Вы должны получить у них соответствующее на это разрешение.
- **Информация о своем точном расположении**
- Старайтесь размещать свои данные (адрес, место работы и т.д.) так, чтобы они не были легкодоступны.
- **Огласка**
- Некоторые сайты и форумы дают Вам ощущение близости. Вы находите людей, близких Вам по интересам и хотите поделиться с ними своим переживаниями или историями из жизни. Однако Вы должны помнить, что форум – это не Ваш дневник, и все, что Вы там напишете, будет доступно обозрению вашей семье, друзьям и детям. Так что, прежде чем размещать какие-либо фото или данные о себе, хорошенько подумайте.

Поведение

Пожалуйста, относитесь друг к другу с уважением. О преследованиях, оскорблениях и размещении негативной информации нужно обязательно сообщать другим пользователям.

Всегда доверяйте своей интуиции: немедленно прекратите переписку с теми, кто Вам кажется неприятным и опасным.

Есть несколько способов защиты информации на вашем компьютере. Например, спам-фильтр уменьшит количество нежелательных сообщений. Антивирусное программное обеспечение может быть использовано для сканирования входящих сообщений.

Если вы получаете на свой адрес информацию, отправитель которой не внушает Вам доверие, сразу удалите файл, чтобы избежать попадания вирусов на компьютер.

Пароли

Выберите пароль, который использует комбинацию букв, цифр и символов. Старайтесь не использовать очевидные слова, например, свою фамилию, или псевдоним, такие даты, как день рождения. Никогда не раскрывайте свой секретный код. Старайтесь не использовать один и тот же пароль на многих сайтах, таким образом, если кто-либо обнаружит один код, он не будет иметь доступ ко всей вашей онлайн деятельности.

Интернет мошенничество

Есть множество видов жульничества в интернете – бизнес-проекты, лотереи, инвестиции, предложения о выгодном сотрудничестве или работе. И подчас трудно определить, где – правда, а где – ложь. Будьте крайне осторожны со сказочно выгодными предложениями, старайтесь не попасться на ловушку мошенников. Храните Ваши личные данные, пароль, номер кредитной карты в безопасном месте и никому не отправляйте эту информацию по электронной почте.

Спасибо за внимание!