

## Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

**Кибермошенничество** – один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое).

**Предупреждение кибермошенничества:**

**Проинформируйте ребенка о самых распространенных методах мошенничества** и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.

Прежде чем совершить покупку в интернет-магазине, **установитесь в его надежности** и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему **простые правила безопасности:**

- Ознакомьтесь с отзывами покупателей
- Проверьте реквизиты и название юридического лица – владельца магазина
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs <http://www.whois-service.ru/>)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить, включая доставку

Объясните ребенку, что **нельзя отправлять слишком много информации о себе** при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды.

**Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.**

## Куда и как обращаться в случаях Интернет мошенничества

### Бесплатный сыр – в мышеловке

На просторах Интернет, все чаще встречаются разговоры о мошеннических схемах в отношении покупателей. Главное - соблюдение одного правила:

Если кто-то обещает вам деньги или другую выгоду, но при этом утверждает, что вам делать ничего не нужно, за исключением внести какую либо сумму предоплаты, то это уже 100% афера.

### Как вернуть свои деньги и наказать мошенника

Если вы уже отдали деньги, то это еще не все потеряно, есть шанс вернуть свое кровное ну или хотя бы наказать обидчика. Наказать тоже польза - чтоб другие не попались на уловку.

Несколько важных аспектов наказания Интернет-мошенников. Можно сразу переходить к действиям или прочитать узнать правила, и не попадаться на «удочку».

Например, если у вас просят сделать перевод через платежную систему QIWI это должно вас насторожить. Причина тому - через эту систему вы никак не вернете деньги.

## **Гарантии от мошенников или сайты однодневки**

На многих сайтах-визитках можно встретить раздел «гарантии», но в большинстве случаев он нужен только для того, чтобы потенциальные покупатели легче расставались с финансовыми средствами. На этой странице все красиво оформлено и расписано о мифических гарантиях. Например, многие вывешивают сканированные копии левых сертификатов чего-либо, свидетельства об аттестации участников, и это может быть картинка с небольшими **photoshop** изменениями.

## **Основная проблема - маленькие суммы**

Понятно, что из-за потери небольших сумм никто не будет обращаться суд. Не всегда понятно кто должен быть ответчиком, отсутствует договор и платежные документы. Даже если решение суда будет в пользу истца, то его почти не реально исполнить, то есть взыскать с ответчика причитающуюся сумму. Более того, эта ситуация негативно сказывается на бизнесе тех, кто ведет дела честно и выполняет все взятые на себя обязательства.

## **Способы противодействия мошенникам**

Самый эффективный способ, это юридическая помощь от профессионалов. Единственной реальной гарантией для покупателя является обращение в правоохранительные органы. Прятки с пробегам и наглые заявления мошенников не отменяют Уголовный кодекс Российской Федерации.

Действия большинства мошенников подпадают под следующие статьи уголовного кодекса Российской Федерации:

- статья 159, «**Мошенничество**»
- статья 171, «**Незаконное предпринимательство**»
- статья 182, «**Заведомо ложная реклама**»
- статья 199, «**Уклонение от уплаты налогов**»
- статья 200, «**Обман потребителей**»
- статья 146, «**Нарушение авторских и смежных прав**»

Многие совершенно ошибочно считают, что **обращение в правоохранительные органы по вопросам мошенничества в Интернете** это сложное, обременительное и наверняка безнадежное мероприятие. Это не так! По времени - **это примерно 15-20 минут, а эффект весьма впечатляющий.**

Обращаться можно по электронной почте! Это значительно упрощает дело. В своем обращении вам достаточно просто сообщить известные вам факты или указать на

подозрительные моменты в коммерческой деятельности. **Все факты и подозрения, указанные в обращениях граждан, обязательно проверяются.** Для большинства Интернет мошенников уже сама проверка становится венцом карьеры.

## **Контакты куда обращаться на Интернет мошенников**

Куда можно обращаться против Интернет-мошенников:

- Обычное заявление в [МВД Российской Федерации](#) (раньше можно было анонимно, но по законодательству МВД не может пустить вход все инструменты отлова мошенников по анонимному запросу - права человека и все такое.)
- Напрямую на [горячую линию МВД](#).
- В [Генеральную Прокуратуру Российской Федерации](#). Если нарушения касается не только [Интернет мошенничества](#), но также стали известны факты мошенничества или нарушения закона должностными лицами.
- Можно также писать в [Федеральную службу безопасности](#) Российской Федерации.

## **Заблуждения**

Беспокоиться о том, что ваши сведения являются неполными или малозначительными не стоит. По вашему обращению состоится проверка и все остальное соответствующие органы выяснят сами.

**Совет.** Обязательно указывайте такой обратный почтовый адрес, с которого вы реально можете забирать почту. Ответы, содержащие информацию о том, какие меры приняты по вашему обращению, всегда приходят только обычной почтой.

Беспокойства о том, что вас могут как-то привлечь к ответственности за ложный донос, беспочвенны. В своем обращении вы просто сообщаете информацию, которую соответствующие органы проверяют, а уже когда что-то выяснится, то по фактам будут возбуждаться и расследоваться уголовные дела, но это уже совершенно не ваша забота.

**Дополнительно.** Расследованием преступлений в сфере высоких технологий в МВД занимается специальное подразделение - Управление «К».

Обратиться в Управление «К» вашего региона очень просто - через любого Интернет провайдера, у них такие контакты есть в обязательном порядке и при необходимости сотрудники регионального Управления «К» передадут сигнал на федеральный уровень.

(Управление «К» по Москве

[http://limited.petrovka38.ru/mvd/structure1/Upravlenija/Upravlenie\\_K\\_MVD\\_Rossii](http://limited.petrovka38.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii) )

**МВД работает и это отлично!** (Пример реагирования МВД)

На телефон поступило сообщение, что моя пластиковая карта заблокирована и указан какой-то телефон, куда перезвонить. Телефон своего банка я знаю отчетливо. На всякий случай проверил работу карты через интернет банк. Все работало.

Но СМС продолжали приходить.

Я написал через онлайн форму в [МВД Российской Федерации](#). Указал свои данные и e-mail, а также своими словами описал ситуацию: кто-то вымогает деньги путем шантажа, телефон такой-то.

На следующий день СМС поступать перестали.

Через три недели я получил официальный ответ по электронной почте, а еще через месяц пришло официальное письмо с подтверждением - официальным ответом МВД на интернет мошенничество.

Сомнения в том, что МВД не работает в данном направлении - беспочвенны.

С первого сентября 2013 года заявление можно написать из личного кабинета [Госуслуг](#), где заполняются автоматически все поля по всей форме.

## Способы найти автора сайта

Используя сервисы WHOIS, например:

- [1whois.ru](#)
- [nic.ru](#)
- [whois.pp.ru](#)
- [wwhois.ru](#)
- [2ip.ru](#)

можно связаться с [хостером](#) или владельцем сайта. С администрацией сайта можно связаться, используя контакты на самом сайте, если таковые имеются.

## Как пожаловаться если сайт распространяет вирусы или спам (spam)

Через E-mail отправьте ссылку (сделайте неактивной ссылкой – только доменное имя или с конкретной страницей при необходимости без протокола) в антивирусные лаборатории, описав причину отправки на английском:

- [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)
- [support@esetnod32.ru](mailto:support@esetnod32.ru)
- [virus@avg.com](mailto:virus@avg.com)
- [virus\\_malware@avira.com](mailto:virus_malware@avira.com)
- [urlsamples@pandasecurity.com](mailto:urlsamples@pandasecurity.com)
- [malware@agnitum.com](mailto:malware@agnitum.com)
- [support@antivirusin.ru](mailto:support@antivirusin.ru)
- [samples@adminus.net](mailto:samples@adminus.net)
- [windexend@submit.microsoft.com](mailto:windexend@submit.microsoft.com)
- [support@emissoft.com](mailto:support@emissoft.com)
- [root@malwares.com](mailto:root@malwares.com)
- [support@nprotect.rsystems.com](mailto:support@nprotect.rsystems.com)

## Куда писать о мошенничестве

Это формы обратной связи, куда можно написать о мошенничестве того или иного сайта. Тем самым вы можете не дожидаться реакции правоохранительных органов, а оперативно

повлиять то, чтобы сайт мошенника больше не был доступен максимальному количеству людей.

- [Yandex AntiSpam](#) - Российская поисковая система.
- [Google](#) - глобальная поисковая система.
- [Baidu](#) - Китайская поисковая система.
- [Scumware](#).
- [Siteadvisor](#).
- [Badwarebusters](#).
- [Cybertopcop](#)s.
- [Trendmicro](#).
- [Cybercrime Tracker](#).
- [Web Inspector](#).
- [Касперский](#) - антивирус.
- [Avira](#) - антивирус.
- [DrWeb](#) - антивирус.
- [Avast](#) - антивирус.
- [Stopbadware](#).
- [Abuse](#).
- [МВД](#) - поддерживается государством.
- [Роскомнадзор](#) - поддерживается государством.
- [Лига безопасного интернета](#) - поддерживается государством.

## **Если материал сайта может нанести вред человеку**

- [МВД](#) - поддерживается государством.
- [Роскомнадзор](#) - поддерживается государством.
- [Лига безопасного интернета](#) - поддерживается государством.
- [Роспотребнадзор](#) - поддерживается государством.
- [Антивирус Касперского](#) - антивирус.

*Галузина Ольга Алексеевна  
ЭКС РО при ДОгМ  
Комиссии по профилактике негативных проявлений  
8 (926) 595 42 32  
nebudzavisim@mail.ru  
www.roditel.educom.ru*