

OUCH!

В ЭТОМ ВЫПУСКЕ...

- Личная безопасность
- Безопасность компьютера
- Информация для родителей

Онлайн игры: правила безопасности

Обзор

Онлайн игры – отличное развлечение, однако они таят в себе ряд специфических рисков. В этом выпуске мы поговорим о том, как защитить себя от опасностей онлайн игр.

Личная безопасность

Онлайн игры доставляют огромное удовольствие, ведь вы можете играть с людьми со всего мира. Но вы никогда не можете знать точно, с кем именно вы играете. Среди любителей игр скрываются и те, кто может серьёзно навредить. Вот некоторые шаги, которые следует предпринять для обеспечения безопасности:

- Будьте внимательны к любым просьбам, требующим от вас действий, например, перехода по ссылке или загрузки файла. Также, как и в случае фишинг атаки по электронной почте, злоумышленники могут попытаться вас обмануть в ходе игры, чтобы заразить компьютер или украсть ваши персональные данные. Если сообщение вам кажется подозрительным, слишком срочным или слишком хорошим, чтобы быть правдой, то, скорее всего, это атака.
- У большинства онлайн игр есть свои рынки, на которых вы можете продавать, менять или даже покупать виртуальные вещи. Также, как и в реальной жизни, в этой системе есть свои мошенники, которые пытаются обманным путём получить ваши реальные или виртуальные деньги. Совершайте сделки с проверенными, надёжными людьми с хорошей репутацией.
- Используйте сильный и надёжный пароль для входа в игровой аккаунт. В этом случае злоумышленникам будет сложно взломать ваш аккаунт, подобрав пароль. Если есть возможность, обязательно используйте двухступенчатую верификацию. Для каждого игрового аккаунта используйте разный пароль. В случае взлома одного из них, остальные по-прежнему будут в безопасности. Сложно запомнить все пароли? Воспользуйтесь менеджером паролей.

Об авторе

Стив Армстронг – основатель фирмы Logically Secure, сертифицированный инструктор Института SANS, и архитектор сервиса CyberCPR (Incident Management Platform). Стив ведёт блог в Twitter: [@Nebulator](#) и сотрудничает со многими ведущими мировыми компаниями-производителями игр, исполняя свои детские мечты и реализуясь профессионально.

Безопасность компьютера

В процессе игры злоумышленники могут попытаться взломать систему или получить контроль над вашим

Онлайн игры: правила безопасности

компьютером. Следующие шаги помогут избежать этого:

- Всегда используйте последнюю версию операционной системы и игровых программ. Устаревшие программы имеют известные уязвимости, которыми могут воспользоваться мошенники для взлома вашей системы. Убедитесь, что вы обновили компьютер и игровые приложения; в последних версиях минимальное количество уязвимостей.
- Используйте антивирус, убедитесь, что он регулярно обновляется и проверяет все файлы на наличие вирусов.
- Загружайте игровые приложения только из надёжных, проверенных источников. Зачастую кибер преступники создают фальшивые или зараженные версии игр, затем распространяют их со своих серверов.
- В игровом сообществе часто разрабатывают дополнительные игровые пакеты с комплектом новых возможностей. Злоумышленники часто распространяют с их помощью вирусы. Также, как и сами игры, дополнительные пакеты следует загружать только из надёжных, проверенных источников. Если какое-либо дополнение запрашивает отключение антивируса или изменение настроек безопасности - не делайте этого.
- Подпольные рынки предлагают многочисленные программы и способы, помогающие мошенничать во время игры. Их не следует покупать не только по этическим соображениям, но и из-за высокой опасности получить вирус. Никогда не устанавливайте программы-мошенники и не используйте сомнительные сайты.
- Внимательно изучите сайты, которыми пользуетесь для игр. Как правило на них есть раздел, посвящённый вашей безопасности и безопасности вашего компьютера.
- На мобильных устройствах следует соблюдать такие же правила, как и для компьютера. Мобильные устройства тоже атакуются кибер мошенниками.



Основы безопасности в онлайн играх – это надёжный пароль, защита вашего компьютера и использование здравого смысла при получении подозрительных сообщений и запросов.

Информация для родителей

Детям следует рассказать о правилах игры онлайн более детально. Информацию следует преподнести в форме диалога, это самый эффективный способ защиты. Один из самых популярных трюков - попросить ребёнка рассказать и показать вам игры, в которые он играет, посмотреть виртуальный мир и понять, что обычно происходит в этих играх. Самый действенный способ – играть вместе. Поговорите с ребёнком о людях, с которыми он общается в

Онлайн игры: правила безопасности

сети. Зачастую игры занимают большую часть социальной жизни детей. Поэтому находясь в курсе событий и ведя диалог, легче всего выявить проблему и решить её наиболее эффективно. Вот некоторые дополнительные шаги:

- Узнать, в какие игры играют ваши дети, соответствуют ли они их возрасту
- Ограничить количество информации, которой можно делиться в сетях. Например, никогда не стоит говорить пароль, возраст, номер телефона или домашний адрес.
- По возможности, разместить игровой компьютер в открытом месте, где вы сможете наблюдать за происходящим. Маленькие дети не должны играть в своей комнате или поздним вечером.
- Издевательства, бранные слова или другие асоциальные привычки тоже могут стать проблемой. Внимательно наблюдайте за ребёнком: если он выглядит подавленным после игры, то, возможно, его там дразнят или издеваются. Если это действительно так, то следует прекратить эту игру и поискать более безопасное окружение или попросить играть только с хорошими друзьями.
- Выясните, поддерживают ли игры вашего ребенка покупки (in-app purchases) и какие функции родительского контроля они предоставляют.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Безопасность домашней сети:	https://securingthehuman.sans.org/ouch/2016#february2016
Социальная инженерия:	https://securingthehuman.sans.org/ouch/2017#january2017
Парольные фразы:	https://securingthehuman.sans.org/ouch/2017#april2017
Менеджер паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется [Creative Commons BY-NC-ND 4.0 license](http://creativecommons.org/licenses/by-nc-nd/4.0/). Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова



securingthehuman.sans.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securethehuman.sans.org)