

OUCH!

В ЭТОМ ВЫПУСКЕ...

- Собственная безопасность
- Защита компьютера/аккаунтов
- Информация для родителей

Безопасность онлайн игр

Обзор

Онлайн игры – отличный способ провести время, однако у них есть свои специфические риски. В этом выпуске мы поговорим о правилах безопасности онлайн игр.

Собственная безопасность

В онлайн играх можно играть и общаться с партнерами по всему миру. Зачастую вы даже не знаете человека, с которым играете. Большинство участников играют для развлечения, но есть и такие, которые хотят навредить. Вот некоторые правила безопасности, которые следует соблюдать.

- Будьте осторожны с сообщениями, которые требуют от вас каких-либо действий, например, перехода по ссылке или загрузки файла. Как и при фишинговой атаке, плохие парни пытаются вас обмануть и заразить ваш компьютер. Любое сообщение, которое требует незамедлительных действий или слишком хорошее, чтобы быть правдой, скорее всего, является атакой.
- Во многих онлайн играх есть свой финансовый рынок, где вы можете продавать, менять и даже покупать виртуальные товары. В виртуальном мире, как и в реальном, есть свои мошенники, которые хотят получить ваши деньги обманным путем или просто украсть их.
- Будьте осторожны с операциями покупки виртуальных товаров за реальные деньги и наоборот. Совершайте подобные операции только на проверенных рынках с хорошей репутацией.
- Ограничьте объем информации, которой вы и ваши дети делитесь в сети. Ни при каких обстоятельствах не публикуйте персональные данные, например, пароль или домашний адрес.
- Многие веб сайты, такие, как онлайн банкинг, используют секретные вопросы для вашей идентификации. Злоумышленники могут попросить ответить на подобные вопросы в игре. Помните, вы не обязаны отвечать на вопросы в играх.

Об авторе

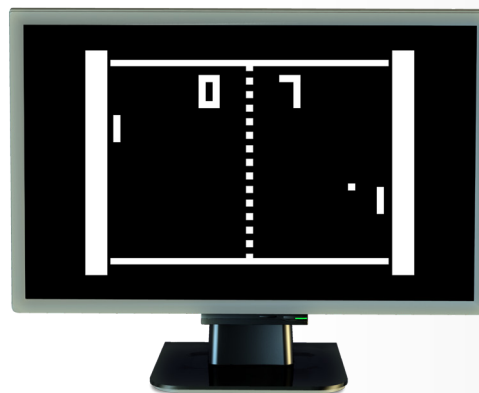
Джейк Уильямс – основатель и консультант компании Rendition InfoSec, лицензированный инструктор и соавтор многих курсов Института SANS. Он ведет записи в Twitter как [@MalwareJake](#) и блог malwarejake.blogspot.com.

Защита компьютера/аккаунтов

Следующим шагом является обеспечение безопасности вашего компьютера. Плохие парни во время игры могут атаковать ваш компьютер или аккаунты; вам следует их защитить.

Безопасность онлайн игр

- Используйте только сильные пароли для компьютера и аккаунта игры. Не допускайте того, чтобы злоумышленники просто угадали или подобрали пароль и овладели вашими аккаунтами. Если есть возможность в игре использовать двухступенчатую верификацию, обязательно воспользуйтесь этим. И последнее: обязательно используйте разные пароли для разных игровых аккаунтов. Если один из них взломают, остальные по-прежнему будут в безопасности.
- Убедитесь, что используете последнюю версию операционной системы и игровых программ. Как и в случае с операционной системой и браузером, устаревшие игровые программы имеют хорошо известные уязвимости, которые могут быть использованы злоумышленниками для получения контроля над вашим компьютером. Своевременно обновляйте компьютер и игровые программы - это защитит вас от большинства угроз.
- Используйте антивирус, убедитесь, что он обновляется и проверяет все файлы, которые вы запускаете, в реальном времени.
- Загружайте игры только из проверенных источников. Если вы загружаете программу для игр, убедитесь, что делаете это с сайта производителя или других известных, проверенных источников. Часто мошенники создают фальшивые и зараженные версии игры и распространяют их со своих серверов. Как только вы их установите, злоумышленники получают полный контроль над вашим компьютером.
- Дополнительные приложения зачастую разрабатываются в игровом сообществе и помогают получить новые возможности в играх. Злоумышленники часто заражают эти приложения, которые с трудом поддаются обнаружению антивирусом. Так же, как и игры, дополнительные приложения следует загружать только из надежных источников. И, наконец, если приложения запрашивают отключение антивируса или изменения в настройках фаерволла, то не стоит их устанавливать.
- Подпольные рынки предлагают огромное количество программ для обмана игр. Помимо того, что это неэтично, большинство программ для обмана игр являются руткитами, одной из опаснейших категорий зловредных программ. Никогда не устанавливайте и не используйте никакие программы для обмана игр.
- Проверьте веб сайты онлайн игр, которыми вы пользуетесь. Многие игровые сайты предоставляют советы по обеспечению вашей безопасности и безопасности ваших устройств. Воспользуйтесь этими советами.
- Если вы пользуетесь мобильным устройством для игр, проявляйте такую же осторожность, как и при игре на компьютере. Кибер преступники уже начали атаковать мобильные устройства.



Чтобы оставаться в безопасности, играя в онлайн игры, используйте сильные пароли, обезопасьте свой компьютер и используйте здравый смысл при общении с незнакомцами или при получении необычных сообщений или вопросов.

Безопасность онлайн игр

Информация для родителей

Если у вас есть дети, удостоверьтесь, что ваши дети следуют советам, приведенным выше. Выполните эти шаги сами, если ваши дети ещё совсем малыши. Обсудите риски с вашими детьми. Образование и открытый диалог с вашими детьми – наиболее эффективные методы их защиты. Один из наших любимых трюков для того, чтобы вывести детей на разговор, заключается в том, что мы просим их показать, как работают их игры, познакомиться с их онлайн-миром. Может быть, даже сыграйте с ними. Наконец, попросите их описать людей, которых они встречают онлайн. Зачастую, онлайн игры являются важной частью социальной жизни вашего ребенка. Разговаривая с детьми (и поощряя их говорить с вами), вы можете обнаружить проблему и защитить детей более эффективно, чем любая технология.

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

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 <http://www.securingthehuman.org>.

Ресурсы

- Социальная инженерия: <http://www.securingthehuman.org/ouch/2014#november2014>
Фишинговые атаки: <http://www.securingthehuman.org/ouch/2013#february2013>
Пароли: <http://www.securingthehuman.org/ouch/2013#october2013>
Что такое антивирус?: <http://www.securingthehuman.org/ouch/2014#december2014>
StaySafe Online: <http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips>
Интерактивные игры: помощь детям сделать игры более безопасными:
<http://www.microsoft.com/ru-ru/security/family-safety/gaming-about.aspx>

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: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова



securingthehuman.org/blog



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



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



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