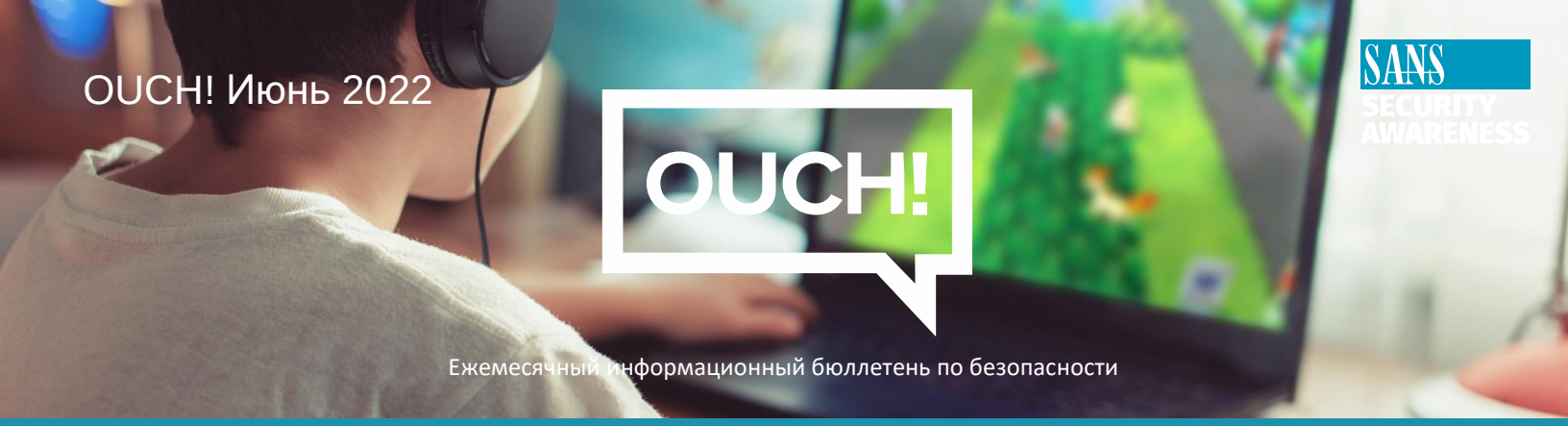
OUCH! Июнь 2022



Ежемесячный информационный бюллетень по безопасности

Безопасная онлайн-игра

Что делает онлайн-игры такими увлекательными, так это то, что вы можете играть и взаимодействовать с другими людьми из любой точки мира, часто вы даже не знаете людей, с которыми играете. В то время как подавляющее большинство людей в сети, как и вы, хотят повеселиться, есть и те, кто хочет причинить вред.

Защита ваших данных

Наибольший риск для онлайн-игр представляет не сама технология, а взаимодействие с незнакомцами.

- Будьте осторожны с любыми сообщениями, которые просят вас выполнить какое-либо действие, например щелкнуть ссылку или загрузить файл. Злоумышленники будут использовать внутриигровые сообщения или фишинговые электронные письма, пытаясь заставить вас предпринять действия, которые могут заразить ваш компьютер, украсть вашу личную информацию или игровые учетные записи. Если сообщение кажется странным, срочным или слишком хорошим, чтобы быть правдой, будьте бдительны, это может быть атака.
- Многие онлайн-игры имеют свои собственные финансовые рынки, где вы можете торговать, обмениваться или покупать виртуальные товары. Как и в реальном мире, есть мошенники, которые попытаются обмануть вас и украсть ваши деньги или любую виртуальную валюту, которая у вас есть. Имейте дело только с теми людьми, которые зарекомендовали себя надежной репутацией.
- Используйте надежный уникальный пароль для любых игровых аккаунтов. Таким образом, злоумышленники не смогут просто угадать ваши пароли и завладеть вашими учетными записями. Если ваша игра/платформа предлагает двухэтапную аутентификацию, используйте ее. Не можете запомнить все свои пароли? Используйте менеджер паролей.

Защита вашей системы

Злоумышленники могут попытаться взломать или захватить компьютер или устройство, на котором вы играете, вам необходимо принять меры для его защиты.

- Защитите свои устройства, всегда используя последнюю версию операционной системы и игрового программного обеспечения или мобильного приложения. Устаревшее программное обеспечение имеет известные уязвимости, которые злоумышленники могут использовать для взлома вашего устройства. Включите автоматическое обновление, если это возможно. Обновляя свои устройства и игровые приложения, вы устраняете большинство известных уязвимостей.
- Загружайте игровое программное обеспечение и пакеты дополнений к играм только с надежных веб-сайтов. Злоумышленники часто создают поддельные или зараженные версии, а затем распространяют их со своего собственного сервера. Кроме того, если какая-либо игра требуют отключения каких-либо инструментов или настроек безопасности, не используйте их.

SANS SECURITY AWARENESS
© SANS Institute 2022

- Возникли подпольные рынки для поддержки мошеннической деятельности. Помимо того, что это неэтично, многие мошеннические программы сами по себе являются вредоносными программами, которые могут заразить ваше устройство. Никогда не устанавливайте и не используйте какое-либо мошенническое программное обеспечение или веб-сайты.
- Проверьте веб-сайт любого программного обеспечения для онлайн-игр, которое вы используете. На многих игровых сайтах есть раздел о том, как обезопасить себя и свою систему.

Для родителей или опекунов

Образование и открытый диалог с вашими детьми — это самый эффективный шаг, который вы можете предпринять для защиты детей. Один из подходов — попросить их показать вам, как работают их игры, показать, как выглядит типичная игра. Возможно, даже поиграть с ними в игру. Кроме того, попросите их описать разных людей, которых они встречают в Интернете. Довольно часто онлайн-игры могут составлять большую часть социальной жизни вашего ребенка. Разговаривая с ними (и они разговаривают с вами), вы можете обнаружить проблему и защитить их гораздо эффективнее, чем любые технологии. Некоторые дополнительные шаги включают в себя:

- Знайте, в какие игры они играют, и убедитесь, что игры соответствуют возрасту вашего ребенка.
- Ограничьте количество информации, которой ваши дети делятся в Интернете. Например, они никогда не должны сообщать свой пароль, возраст, номер телефона или домашний адрес.
- Подумайте о том, чтобы их игровое устройство находилось на открытом месте, где вы могли бы видеть их. Кроме того, младшим детям не следует играть поздно ночью и в своих комнатах.
- Запугивание, нецензурная брань или другое антиобщественное поведение могут стать проблемой. Следите за своими детьми, если они выглядят расстроенными после игры, над ними могли издеваться в сети. Если над ними издеваются в сети, сообщите об этом на игровой сайт и дайте им возможность играть в онлайн-игры только с надежными друзьями.
- Узнайте, поддерживают ли игры вашего ребенка покупки в приложении и какие виды родительского контроля они предоставляют.

Приглашенный редактор

Чарли Голднер — основатель CyberNV и инструктор SANS. Он активен в LinkedIn и поддерживает государственные учреждения. На протяжении многих лет он провел много часов за играми на ПК и консолях.

Ресурсы

Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Многофакторная аутентификация: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Менеджеры паролей: : https://www.sans.org/newsletters/ouch/password-managers/
Интернет-безопасность для детей:: https://www.sans.org/newsletters/ouch/online-security-kids/

Роман Полаков

OUCH! Публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. . Вы можете делиться или распространять этот информационный бюллетень, если вы не продаете и не модифицируете его. Редакционная коллегия: Уолтер Скривенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг.