Полезная информация и советы по интернет-безопасности

Что такое Malware (Малварь) и как обезопасить себя от кибер-угроз?

Malware или **Малварь** - вредоносная программа, цель которой нанести ущерб пользователю или компьютеру и его содержимому. **Малварь** - общее название для всех видов кибер-угроз, таких как: вирусы, трояны, шпионские программы, кейлоггеры, adware и др. **Malware** или вредоносы - достаточно распространенный вид кибер-угроз, и столкнуться с ними может каждый.

Какой вред может причинить Malware моему компьютеру?

- Изменить настройки браузера и не дать изменить их пользователю (например, устанавливает новую домашнюю страницу или поиск по умолчанию);
- Истратить ресурсы компьютера, тем самым снизить его быстродействие;
- Установить рекламные программы на компьютер, такие как всплывающие окна и баннеры, которые работают даже без подключения к интернету;
- Использовать компьютер и его ресурсы для DDoS-атак или майнинга криптовалют;
- Заблокировать доступ к сайтам антивирусов и другим сайтам, содержащим инструменты для борьбы с вредоносным ПО;
- Собрать личные данные пользователя: логины, пароли, номера банковских карт и прочее;
- Без ведома пользователя скачать с интернета и установить другое вредоносное ПО.

Как удалить Malware с компьютера?

Такая программа хорошо маскируется и может ничем не выдавать свое присутствие для пользователя. Сегодня существует множество программных инструментов, чтобы очистить компьютер от Malware - антивирусы и специализированные Anti-Malware программы. Однако многие вредоносные программы обладают настолько высокой степенью защиты, что их практически невозможно удалить после запуска.

Как SkyDNS блокирует доступ к ресурсам, содержащим Malware?

SkyDNS предлагает альтернативный способ избежать вредоносных программ. Наша система аналитики, основанная на принципах машинного обучения, позволяет с точностью до 98% определять ресурсы, содержащие вредоносное ПО и эффективно блокировать доступ к ним. Предотвратите негативное влияние Malware еще до того, как вредоносная програма попадет на ваш компьютер.

Что такое фишинг и как защититься от кражи паролей в интернете?

Фишинг — это вид интернет-мошенничества, основанный на невнимательности пользователей в Сети. Чтобы вытянуть из пользователей личные данные, логины, пароли, номера банковских карт или другую важную информацию, злоумышленники создают поддельные страницы сайтов магазинов, банков, почтовых клиентов и соцсетей. Визуально они не отличаются от оригинальных, поэтому невнимательный посетитель вводит свои данные авторизации, после чего они попадают к мошенникам. Таким образом, мошенники могут взломать страницу вконтакте с помощью фишинга или получить доступ к банковскому аккаунту своей жертвы.

Как обеспечить защиту от фишинга?

Прежде всего, не доверяйте сообщениям, поступающим на вашу электронную почту, и не переходите по ссылкам, указанным в письме! Банки и соцсети не занимаются рассылкой по почте в случае проблем с аккаунтом. Никогда не вводите свои конфиденциальные данные на домены, начинающиеся с http:// (то есть незащищенные домены), следите, чтобы адрес сайта начинался с безопасного протокола https://.

Надежный способ защитить себя от фишинговой атаки - установить контент-фильтр SkyDNS. Благодаря нашему сервису вы можете быть уверены, что ваши личные данные и пароли не «утекут» к мошенникам.

Как проверить сайт на фишинг?

Не уверены в безопасности страницы? На сайте SkyDNS вы можете проверить сайт на фишинг:

1. Перейдите в форму проверки: https://www.skydns.ru/check/.
2. Скопируйте подозрительную ссылку и вставьте ее в нужное поле.
3. Сервис автоматически определит принадлежность сайта к той или иной категории.

Куда сообщить о фишинговом сайте?

Если вы обнаружили подозрительный сайт, отличающийся от оригинала внешне или в адресной строке, сообщите об этом:

- владельцу или администрации ресурса;
- support@skydns.ru. Мы включим сайт в список блокировки

Как заблокировать рекламу?

Что раздражает нас в интернете больше всего? Правильно, реклама. Она навязчиво предлагает что-либо купить, поиграть в онлайн-казино или потратить время на чтение бесполезных статей о «методе похудения Пугачевой». Здесь мы расскажем об основных видах интернет-рекламы и как с ней бороться:

1. **Баннеры.** Один из самых простых видов онлайн-рекламы - ссылка на сайт, оформленный в виде картинки-баннера.
2. **Всплывающие окна.** Наиболее раздражающая реклама. Иногда закрывает значительное пространство страницы сайта, что затрудняет чтение основного контента. Также могут быть выполнены с использованием технологии flash и иметь звуковую составляющую (зачастую, очень громкую). Не всегда просто закрыть всплывающее окно: разработчики онлайн-рекламы специально помещают кнопку закрытия в самом неподходящем месте и делают ее максимально незаметной.
3. **Контекстная реклама.** Основана на ранее сделанных вами запросах в поисковых системах. Если вы когда-либо искали «где купить пиццу?» в интернете - не удивляйтесь потом, что рекламные предложения пиццерий будут преследовать вас на каждом шагу.
4. **Аудио- и видеореклама.** Видео-ролики, которые вы обязаны просматривать в течение 10-30 секунд, прежде чем сможете закрыть их и перейти к основному содержанию страницы. Иногда можно посмотреть один рекламный ролик, но когда приходится смотреть по 20-30 роликов за час (возможно, совершенно одинаковых), это раздражает.
5. **Реклама в мобильных приложениях и играх.** Особенно раздражает реклама в тех приложениях, которые мы используем ежедневно (например, Скайп или YouTube). Рекламные баннеры в играх легко убрать, но за это разработчики потребуют с вас денег.

Реклама не только отвлекает вас от непосредственных задач интернет-серфинга, но и значительно замедляет работу браузера и всей системы в целом. Особенно сильно расходует ресурсы компьютера видео-реклама и реклама, использующая flash-технологию. Также следует опасаться, что кликнув по баннеру (случайно или намеренно), можно заразить свой компьютер вредоносным ПО или перейти на фишинговый сайт.

Как убрать рекламу на компьютере?

Заблокировать рекламу можно с помощью специальных программ или плагинов от рекламы для браузера. Однако маркетинговые технологии не стоят на месте, и разработчики онлайн-

рекламы находят все новые и новые способы, чтобы обходить блокировку.

Рекламный фильтр встроен в **сервис контент-фильтрации SkyDNS** по умолчанию, как одна из опций на тарифах SkyDNS.Семейный, SkyDNS.Образование и НКО, SkyDNS.Бизнес. ??? ???? ?? ????? ???????? ? ??????????? ???????? — ??????????? ?? 90% ???? ????? ???????: ?? ???????? ? ??????????? ????, ?? ??????????? ? ????????????. Наше решение позволит убрать онлайн-рекламу без установки дополнительных програм на компьютер или плагина для браузера.

Как убрать рекламу из приложений?

Облачный фильтр интернета SkyDNS дает возможность убрать рекламу не только на компьютере, но и на любых устройствах, подключенных к сети Wi-Fi, в том числе и рекламу в играх и приложениях на планшетах и телефонах.

Блокировка по разрешающему и запрещающему спискам

Как работают разрешающие и запрещающие списки?

?? ?????? ????????? ?????????? ????????? ?????? ?? ????? ???????????? ? ?????.

Запрещающий список позволяет блокировать определенные домены. Например, можно не блокировать всю категорию «Социальные сети», а заблокировать только какую-нибудь конкретную соцсеть.

Разрешающий список действует наоборот — вы блокируете всю категорию целиком, но вносите исключения из данной категории, которые блокироваться не будут. Функция **Работать по разрешаему списку** особенно полезна для домашних пользователей и школ, так как позволяет переходить только на сайты из разрешающего списка, остальные сайты блокируются.

Как добавить сайт в разрешающий или запрещающий список?

Чтобы пользоваться функцией списков исключений, зарегистрируйтесь на нашем сайте, затем создайте списки и добавьте домены в соответствующие поля по очереди. Системе потребуется до 15 минут, чтобы внести изменения на сервер. После этого список исключений будет работать. Следует помнить, что размер запрещающих и разрешающих списков различается, в зависимости от тарифа.