

ВНИМАНИЕ, ОПАСНОСТЬ!

ВРЕДОНОСНЫЕ РАСШИРЕНИЯ ДЛЯ БРАУЗЕРОВ!

ЧТО УМЕЮТ ДЕЛАТЬ ВИРУСНЫЕ РАСШИРЕНИЯ?

- Размещать навязчивую рекламу в вашем браузере
- Совершать действия от имени пользователя в соцсетях (лайкать нужные материалы, делать рекламные посты)
- Перенаправлять на фишинговые или зараженные сайты
- Незаметно для пользователя кликать на вредоносные или рекламные ссылки, активировать скрипты
- Подсовывать пользователю для скачивания вирусное ПО, или веб-приложения
- Самовосстанавливаться после удаления
- Подменять контент, видоизменять кнопки, интерфейс страницы, оформление
- Следить за серфингом пользователя в интернете: куда он ходит, какие сайты посещает, чем интересуется



КАК ОНИ ПОПАДАЮТ В ВАШ КОМПЬЮТЕР?

- В комплекте с другими программами (“в нагрузку” с какими-то нужным файлом или программой)
- Выдает себя за полезное ПО (наряду с полезными функциями программа может иметь и несколько “неполезных”)
- Обманом и шантажом (мошенники не дают пользователю уйти с их сайта, пока тот не установит программу или приложение)

В КАКИХ БРАУЗЕРАХ ОНИ УСТАНАВЛИВАЮТСЯ?

Дополнительные расширения поддерживают такие браузеры:

GOOGLE CHROME

OPERA

MOZILLA FIREFOX

EDGE

SAFARI

ЯНДЕКС.БРАУЗЕР

INTERNET EXPLORER

AMIGO, и др.



КАК ЗАЩИТИТЬСЯ ОТ "ВРЕДОНОСА"?



- Внимательно следить за ПО, которое устанавливаете
- Устанавливайте расширения **ТОЛЬКО** из официальных источников!
- Проверяйте права доступа, которые запрашивает приложение
- Используйте браузер со встроенной защитой
- Быть бдительным при открытии файлов *.exe, .vbs, .scr
- Удалите все подозрительные файлы и расширения, затем просканируйте компьютер
- Если расширение появляется и после удаления - удалите приложение и создайте новый ярлык браузера
- Обновите антивирус и просканируйте компьютер. Если антивирус не помог - восстановите систему до более ранней версии
- В крайнем случае, напишите разработчику браузера

**ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**

