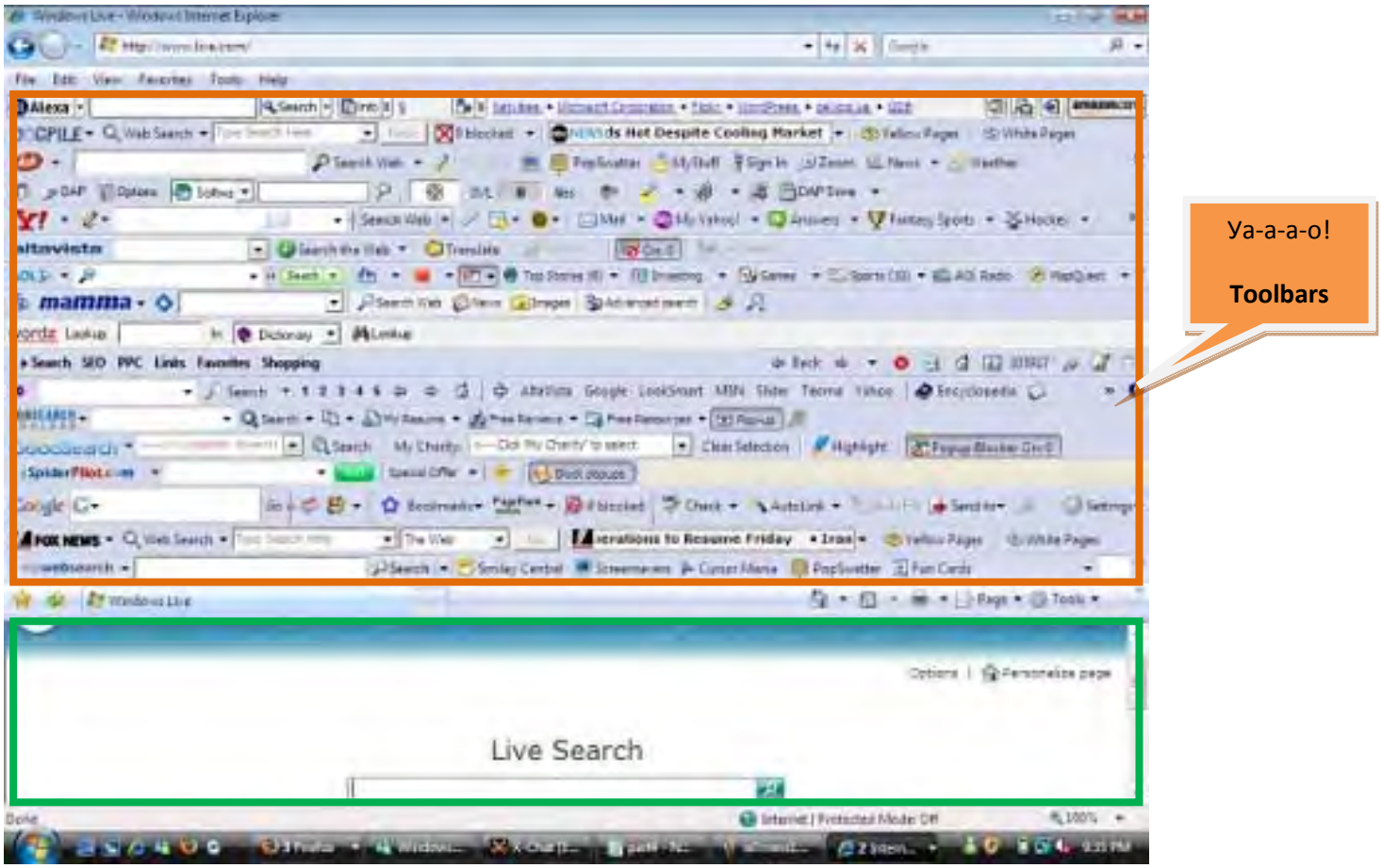
Рискове при изтегляне и инсталиране на свободен софтуер

от Chad Whitley на 12.02.2011

Наскоро написах една статия за най-добрите скрийнсейвъри. Нещото което научих, докато я писах е това, че наистина трябва да бъдем твърде много внимателни, когато възнамеряваме да инсталираме нов софтуер. В тази статия ще използвам това, което съм научил при търсене/намиране на нови скрийнсейвъри като пример за рисковете с всеки нов файл Софтуер добавен във вашата система. Добавил съм и съвети за да изградите система която да сведе до минимум тези опасности! Описвам тези рискове за „отваряне на очите" и се надявам, че „споделянето" ще бъде полезно в нет-лова за софтуер.

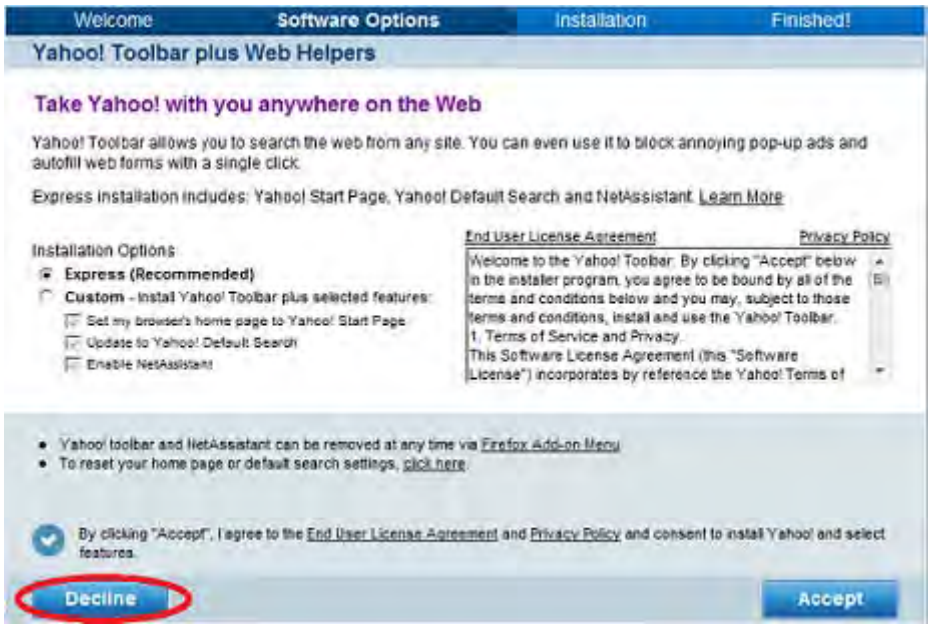
Toolbars – Инструментални ленти

Лентите с инструменти може да откраднат информационна площ! Дори доста полезните от тях могат да претрупват браузъра с излишно присъствие, ако не сте внимателни.... В крайна сметка, може да бъдете изправени пред ситуация, в която виждате повече ленти с инструменти в прозореца на браузера ви, отколкото действителното съдържание на страниците в посещаваните уебсайтове. (долната илюстрация)



Много от свободния (безплатен) софтуер (скрийнсейвъри, торенти, антивируси, тулове, оптимизатори, плеяри, за монтиране на образи и мн. др.) *ще се опита да ви принуди или подмами* да приемете инсталирането на лента(и) с инструменти. Почти винаги софтуерът е безплатен затова, защото рекламодатели инвестират в разработката му с добавки и подхлъзване за инсталиране на лента с инструменти при инсталацията в техен интерес. Винаги четете

внимателно какво се инсталира и... *не забравяйте да махнете или откажете оферти за инсталирането на ленти с инструменти*, които всъщност няма да използвате много. Обикновено приемането на лента с инструменти ще бъде избран по подразбиране в някой от диалоговите прозорци по време на инсталацията на „безплатния“ софтуер , така че наистина трябва да бъдете внимателни и да следите за предлагането им.



Някои софтуери направо ще изискват от вас да приемете лента с инструменти, за да се инсталира безплатния софтуер. Уверете се, че наистина искате такъв безплатен софтуер, защото за съжаление понякога за повечето ленти с инструменти, след като те са били инсталирани, може да се окаже доста трудно да се отървете от тях в последствие. (пр. ленти за промяна на търсачката по подразбиране) !

Нежелан софтуер и Оферти

Освен ленти с инструменти, има и други видове НЕЖЕЛАН софтуер, който се предлага „услужливо“ или е прихлъзнат сенчесто, ей така, при инсталиране на НОВ софтуер. Те могат да ви се „натресат-добавят“ с различни видове безплатен софтуер. Тук ще спомена най-често срещаните случаи.

FRENDS Често срещан случай е софтуер "приятел", като нашия приятел-долу, който би трябвало да ви помага да използвате по-добре компютъра си ... но е по-агресивен, любопитен и разсейващ отколкото сте очаквали. Пр. скандалния BonziBUDDY . Подобни програми-***приятели*** много вероятно съдържат **зловреден софтуер**.

BROWSERS Друг вид **агресор** са непознатите ***браузъри*** (понякога умишлено създадени), които лесно биха могли да бъдат премахнати, но включват нежелани парчета функционалност, които правят неща, нежелани от вас докато се инсталират (или са стартирани) в т.ч. следят вашата дейност или ви „крадат“ лична информация. Ако ви се предложи избор за инсталация на нов браузър, то много по-безопасно е да отидете директно към сайта на разработчици на най-популярните Google Chrome, Internet Explorer или Mozilla Firefox, отколкото да приемете инсталирането на този, който ви се предлага в пакет с друг софтуер.

TRIALS Разновидности на ***пробен*** софтуер също често се предлага. Обичайно GAMES игри, които могат да изискват допълнителна покупка, за да продължите примерно в нивата на играта.

GUARDS Друг пример са предложенията за ***пробна*** инсталация на системи за сигурност – ***охранители***: защитни стени (firewalls), антивирусни програми (antivirus), оптимизатори (tools). Тук трябва да бъдете също много внимателни, особено ако вече имате друга инсталирана програма с подобни функции за сигурност. Като правило две решения за сигурност с покриваща се функционалност, когато се използват... водят до конфликти и системни сривове и са с клоняща към 0% сигурност. Точно както с браузърите, по-добре е да се направи информиран избор и да изтеглите и инсталирате решения за сигурност от официалния уеб-сайт, вместо да се използва това, което се предлага в пакет с друг софтуер.

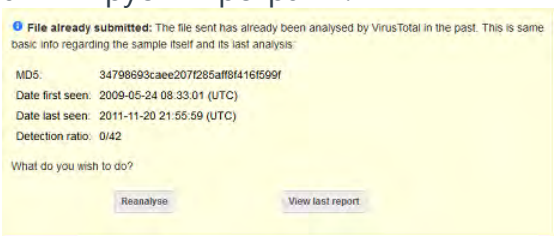
още **ПОДХЛЪЗВАНИЯ**... Някой безплатен софтуер може да поиска от вас да обявите своя е-мейл (***спам*** – никой няма да ви каже че ще ви спамира пощата с нежелани чести съобщения, но е много вероятно да използват мейла ви в този контекст от свое име или да го предостави за Adware цели) ***или***... с предложение да промените *Home Page* с адрес на страницата на техен (или на рекламодател) сайт ***или***... да се възползвате от други *промоции*, за ***да се насладите на безплатния софтуер*** ;-) Рискът при избора е ваш! Бъдете внимателни!

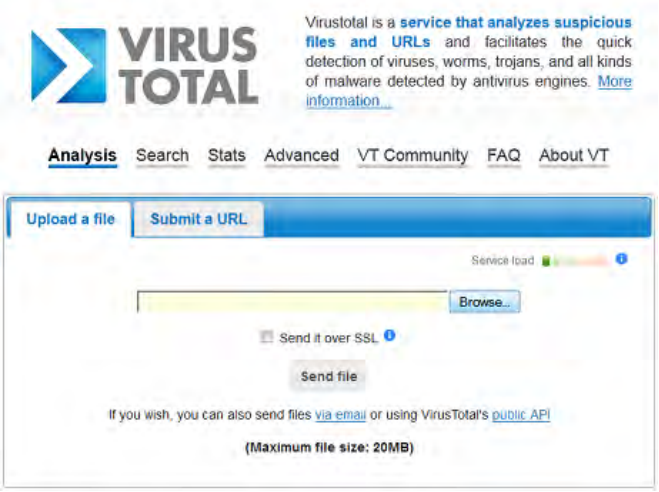
Вируси, Троянски коне и Adware (рекламен софтуер)

Това са допълнителните скрити рискове, които поемате при инсталирането на всеки нов софтуер който сваляте. **Наличието на работещ антивирусен софтуер (актуални вирусни сигнатури) на вашия компютър е задължително условие за избягване на рисковете от тях!** Аз препоръчвам да разгледате нашата статия Сигурност за всички по темата.

За допълнително ниво на защита, препоръчвам да сканирате с антивирусната си програма всеки файл който изтегляте, преди да го инсталирате! Друг начин, по който можете да се застраховате от рискове е с помощта на удобна малка уеб услуга, наречена Virus Total . По принцип, като отидете на сайта ще трябва да качите „сваления" от вас файл за проверка преди да го инсталирате на вашия компютър!

Услугата ще ви информира, ако някой друг е качил същия файл, в случай, че в него е открито нещо нередно. Ще откриете, че най-популярните файлове там са качени поне веднъж преди вас. Можете да го проверите с по-известните антивирусни програми!





И накрая, тя ще ви даде възможност да оставяте коментари и информация за други потребители на дадения файл. Ако възнамеряваш да се възползват от тази възможност, не забравяй да си създадеш акаунт за *Virus Total* ! Като успокоително предупреждение! Ако само някоя(и) от по-малко известните антивирусни програми са намерили нещо подозрително в даден файл, той може да се използва и вероятно тревогата е фалшива! Доверявайте се повече на по-популярни и авторитетни Антивируси!

Заключение

Реших че споделянето може да ви е полезно!. Вие също можете да споделяте вашия опит по изпробване на нови програми!