**8 съвета на специалисти в бранша**

**|Как да предпазим компютъра си от вируси?**

[**https://trierrasoft.com/8-stapki-da-predpazim-pc-ot-virusi/**](https://trierrasoft.com/8-stapki-da-predpazim-pc-ot-virusi/)

ПУБЛИКУВАНО НА [16/06/2021](https://trierrasoft.com/8-stapki-da-predpazim-pc-ot-virusi/) ОТ [TRIERRA SOFT](https://trierrasoft.com/author/trierrasoft/)

**16  
Юни**

*Ще ви покажем как да предотвратите заразяване с вирус, като спазвате 8 лесни правила по време на работа. Най-добрата защита е превенцията, а тя е възможна само когато сме добре информирани.*

Знаете ли коя е най-голямата заплаха за компютъра ви? Вие.

Когато става въпрос за заразяване с вирус, човешкият фактор е този, който изиграва най-значима роля. Защо? Нека обясним.

**В какво се състои заплахата?**

Компютрите са неизменна част от ежедневието ни. Колкото по-популярни стават, толкова по-повече измами ни атакуват ежедневно. Всеки ден делим едно общо работно място с всички злонамерени софтуери, вируси, криптовируси, хакери. Споменатите имат различни цели:

* Да навредят на файловете ви – криптовирусите имат за цел да направят информацията ви нечетима до изплащането на откуп;
* Кражба на лични данни – освен данните на банковите ви сметки и карти, вече често виждаме и кражба на информация за социални статуси, адреси, телефони, пощи, социална сигурност и т.н.;
* Да направят системата ви бавна и неизползваема – срещали сме вируси, които са на практика безпредметни и единствено блокират огромен ресурс и забавят производителността на компютъра ви;
* Натрапване на нежелани реклами и антивирусни от 3-ти лица – да, понякога вирусите се крият в антивирусната система.

Независимо каква е мисията на вируса, нека ви спестим главоболия като ви запознаем с нашите 8 съвета как да предотвратите заразяване на компютъра си с вирус:

1. **Винаги обновявайте Windows до последна версия**

Сещате се за тези досадни напомняния от Windows, който непрекъснато ви агитира да обновите системата си до последна версия. Повечето пъти това не е без причина. Windows ежедневно събират информация за най-новите вируси и заплахи на платформата им – все пак почти 90% от потребителите на компютри използват именно тази операционна система. Затова, може би ви се струва често, но всяка седмица от Microsoft пускат нови и нови ъпдейти. Рано или късно, редно е да ги изтърпите.

Да не споменаваме, че немалка част от проблемите, които имате със системата биват оправяни периодично и е във ваш интерес да използвате най-новата възможна версия.

1. **Не отваряйте линкове от имейли**

Няма по-лесен начин за заразяване с вирус от линк в съмнителен имейл. Често нападателите използват познати имена на пощи и удобни заглавия. Могат да се представят за банката ви, която иска да промените паролата си с цел сигурност. Други пък ви доставят пратката, която чакате и можете да проследите в предоставения линк.

В последно време организации като банки, пощи, куриери и онлайн магазини избягват да слагат линкове в имейлите си, за да не бъдат бъркани с фалшивите такива.

Внимателно разгледайте изпращача – обикновено си проличава още като видите името на домейна, от който е изпратен (името изписано след @).

**Пример:**

[communication@unicreditbulbank.info](mailto:communication@unicreditbulbank.info) – Това е истински имейл адрес, няма повод за притеснение

[communication@uncrdtbulbank.info](mailto:communication@uncrdtbulbank.info) – Забелязвате ли нещо?

Фирмите занимаващи се със защита от вируси и антивирусни системи наскоро ни обърнаха внимание, че много хакери се възползват от възможността да напишеш две идентични на вид букви, веднъж на кирилица и веднъж на латиница. Такива са „о,е,р,х,а,с,у“.

Открийте разликите:

Speedy

Sрееdу

Вероятно не я виждате, но вторият път Speedy е изписано с 4 букви на кирилица и няма нищо общо с първото изписване освен визуално.

В случай, че имате съмнение за подобна злоупотреба и евентуален вирус, копирайте имейл адреса на изпращача и го сложете в текстов редактор с корекция за правопис, например Word. Той ще подчертае думата като непозната.

1. **Използвайте антивирусна система**

Безплатните антивирусни системи не са особено сигурни. Ако не ви се плаща годишна такса за платена, практиката ни показва, че вградената в Windows 10 е по-добра от която и да е ограничена безплатна версия на платен софтуер.

Ако става въпрос за работния ви компютър и не желаете някой да посегне на файловете ви, които са изключително важни, то най-добре отделете малка част от бюджета си и инвестирайте в качествена антивирусна система. Ние сме представители на [NOD32](https://www.eset.com/bg/), чиято такса е символична и е на годишна база в зависимост от нивото на сигурност, което изберете.

Най-популярният и коварен вирус е **криптовируса**, който е способен да унищожи безвъзвратно цялата ви информация. Още ли се колебаете дали да закупите антивирусна система?

1. **Правете резервни backup-и периодично**

Всеки ден, всеки 3 дни, всяка седмица или всеки месец, резервните копия (backup-и) на файловете ви е най-добрата защита срещу вируси.

Винаги когато създавате поредния работен документ или качвате снимките на детето си от фотоапарата на компютъра се запитайте колко важна е информацията за вас. Ако отговорът е „без нея не мога“, значи трябва да я имате на поне 2-3 места. Запишете я на флашка, на външен хард диск, на друг компютър, в Google Drive или който и да е безплатен онлайн ресурс.

Никога не разчитайте само на 1 копие от вашата жизненоважна информация!

1. **Използвайте сигурна парола**

„12345678“ „име123“ и рождената дата не са най-подходящия избор за пароли. Алгоритъм за разбиване на пароли би могъл да ги разгадае за минути, да не говорим, че някой с повече късмет може да ги налучка доста лесно.

**Коя парола е сигурна?**

Сигурната парола съдържа:

1. Поне 1 главна буква.
2. Повече от 1 малка бука.
3. Поне 1 цифра.
4. Поне 1 специален символ (#@$%^&\*!).
5. Съдържа микс от изброеното с поне 8 символа.

Ако защитавате важна информация, добре е да не използвате една и съща парола за всичките си акаунти в интернет.

**Съвет:** Сложете 1-2 букви в паролата си, които да бъдат различни за всеки ваш акаунт (например, паролата за facebook да има fb в края, за пощата – ml, за Instagram – ig).

Има удобни безплатни софтуери, които помнят паролите ви вместо вас. Достатъчно е да запомните само 1 парола, която отключва всички останали. Само внимавайте да не я забравите!

1. **Периодично проверявайте системата за вируси**

**Как?**

Достатъчно е просто да стартирате сканиране за вируси през вашата антивирусна система.

**Колко често?**

Препоръчително е поне веднъж в седмицата да правите проверка за вируси.

**Кога е удачно да се прави?**

Най-подходящият момент е точно преди да направите backup, за да сте сигурни, че файловете, които спасявате не съдържат вирус.

1. **Внимавайте какво изтегляте**

Винаги използвайте добре защитен браузър когато сваляте файлове от интернет (Chrome, Mozilla Firefox, Edge, Opera, Safari). Ако някой сайт ви се струва подозрителен – има текстове на различни езици, бутоните за „Изтегляне“ са повече от 1 и др., най-добре не рискувайте.

Дори да сканирате изтегления файл за вируси, често пъти при инсталационните файлове заплахата се крие по време на инсталацията. Внимателно четете какви въпроси ви задава инсталатора, какви отметки има и какво ви подканва да изтеглите като допълнителен софтуер.

Ако се усъмните във изтеглен файл, най-добре го прекъснете още на фаза изтегляне. В случай, че вече е изтеглен, изтрийте го перманентно (Shift+Del).

1. **Използвайте Ad Blocker**

Сигурно сте чували за него, Ad Block или Ad Blocker е безплатна добавка към браузърите, която блокира изкачащите прозорци ( pop-ups ). Можете да я изтеглите от „Магазините“ App Store на всеки от браузърите. Ad Block ви позволява да избирате измежду няколко нива на защита, като ограничава изкачащите прозорци и блокира рекламите на територията на сайта, който посещавате.

Изкачащите прозорци са опасни, защото ви се появяват непрекъснато и е възможно да кликнете на злонамерен бутон погрешка. Досадни са и почти винаги рекламират или предлагат неадекватен продукт или услуга за вашите интереси.

**Как да разберете дали компютърът ви е заразен с вирус?**

Сред най-често срещаните проблеми са:

* Честа поява на изкачащи (pop-up) прозорци. Обикновено те ви агитират да си изтеглите антивирусна система или друг софтуер, но не се подлъгвайте.
* Промяна на началната страница като отворите браузър. Ако заглавната страница ви се стори различна или непозната, вероятно компютърът ви е заразен с вирус.
* Рекламни имейли изпратени от ваше име към вашите контакти. Промяна на паролата на мейла не е достатъчна мярка. Трябва да се обърнете към специалисти или да пробвате със сканиране на антивирусна система.
* Често изключване на компютъра или забиване/замръзване на екрана. Нелогично и необичайно поведение на операционната система при ежедневна работа.
* Бавно и затруднено бързодействие на компютъра. Резки спадове в производителността на системата могат да сигнализират за вирус.
* Ако ви се налага да затваряте програми при стартиране на операционната система е възможно да имате вирус.

Ако имате подозрения, че компютърът ви е заразен с вирус, няма място за притеснение. [Доверете се на специалисти](https://trierrasoft.com/serviz/) и се уверете, че информацията ви е спасена на поне 2 места.

В заключение, злоупотребите в интернет и заразяването с вируси е все по-често срещано явление в наши дни. Вземете всички необходими мерки и бъдете внимателни при работа в интернет. Ако имате нужда от помощ, ние сме насреща!