



## [Cum Ă®Ăfi protejezi computerul Ă®mpotriva noului virus ransomware GoldenEye / Petya](#)

Category : [Tutoriale Recenzii](#)

Publicat de admin in 28-Jun-2017 12:05

GoldenEye este o noua versiune a unui virus de tip ransomware care cripteaza fiĂşierele Ăşi blocheazĂş accesul la computerul tĂşu iar pentru deblocare solicitĂş o sumĂş de bani. Virusul GoldenEye se rĂşspĂşndeĂşte rapid, Ăn ultima zi atacĂşnd zeci de mii de computere din toata lumea.

Primul sfat pentru a nu exista riscul sĂş Ăşfi infectezi computerul este sĂş nu deschizi mailurile primite de la persoane necunoscute, mailurile suspecte, ataĂşamentele lor Ăşi spamurile. SĂş nu instalezi niciodatĂş nici un fiĂşier necunoscut primit pe email, chiar dacĂş poate pĂşrea ca este primit de la o cineva cunoscut.

Al doilea sfat este sĂş Ăşfi actualizezi Windows-ul Ăşi sĂş ai instalat un program antivirus care protejeazĂş Ămpotriva viruĂşilor de tip ransomware. Ăn continuare iDownload.ro va ofera pentru download cĂşteva programe antivirus gratuite care Ăşfi poate proteja computerul in cazul Ămpotriva viruĂşilor de tip ransomware.

[Bitdefender Anti-Ransomware Tool \(gratuit\) - download](#)

[Malwarebytes Anti-Ransomware \(gratuit\) - download](#)

[Bitdefender Antivirus Free Edition \(gratuit\) - download](#)

[HitmanPro.Alert \(30 zile gratuit \)- download](#)

Ce faci dac  computerul t u a fost infectat cu un virus ransomware GoldenEye?

 n cazul  n care computerul t u a fost infectat cu acest virus iar fi ierele sunt blocate exist  cateva posibilitati de a- ei recuperarea fi ierele f r s  pl te ti suma cerut  de infractori.

Porne te computerul  n Safe Mode with Networking,  n Windows XP si 7 apas  F8 de mai multe ori  n timp ce porne te computerul.

 n Windows 8 intra in Safe Mode with Networking urmand urmatorii pasi: "General PC Settings"

selectezi "Advanced startup". Click pe "Restart now" computerul va reporni cu meniul "Advanced Startup options". Click pe "Troubleshoot" si apoi click pe "Advanced options" apoi click pe "Startup settings". AZpesi butonul si computerul va reporni si va afisa pe ecran Startup Settings

apesi F5 pentru a porni computerul in Safe Mode with Networking.

Apoi poti deschide un browser si poti descarca un program din cele de mai sus pentru scanarea computerului si pentru eliminarea virusului.

O alt  variant  de  tergere a virusului este de a utiliza "Safe Mode with Command Prompt"  i

"System Restore" pentru restaurarea sistemului la o dat  anterioar  infectarii cu GoldenEye. C nd porne te computerul apas  F8, apare o fereastr  "Advanced Boot Options", selectezi din tastatur  "Safe Mode with Command Prompt" si apesi Enter.

Se deschide o nou  fereastr  Command Prompt scrii cd restore  i apesi Enter.

Apoi apare fereastra System Restore unde dai NExt si alegi restaurarea sistemului la o data anterioara infectarii cu virusul ransomware. Dupa restaurarea sistemului scaneaza si dezinfecteaza computerul cu unul din programele antivirus de mai sus.

Pentru restaurarea unui anumit fisier poti incerca urmatoarea varianta manuala de de recuperare.

Daca exista un backup al fisierelor functioneaza cu un click dreapta > Properties > selectezi tabul Previous Versions si apoi apesi butonul "Restore".

 n func ie de versiunea virusului GoldenEye care va afecteaza computerul trebuie sa precizam ca solutiile de mai sus nu functioneaza in toate cazurile. Datorita

faptului ca virusul se modifica rapid sau cei care l-au creat l-au modificat poate bloca accesul la anumite setari din Windows pentru a preveni Återgerea lui.

Cu toate cÄ existÄ diferite posibilitaÅei de eliminare a virusului GoldenEye trebuie sÄ Åitii cÄ cea mai buna protecÅie este prevenirea infectÄrii computerului. Chiar dacÄ reuseÅti sÄ elimini infecÅia acestui virus, recuperarea fiÅierelor poate fi foarte dificilÄ sau imposibilÄ datoritÄ algoritmului foarte puternic de criptare a fisierelor.