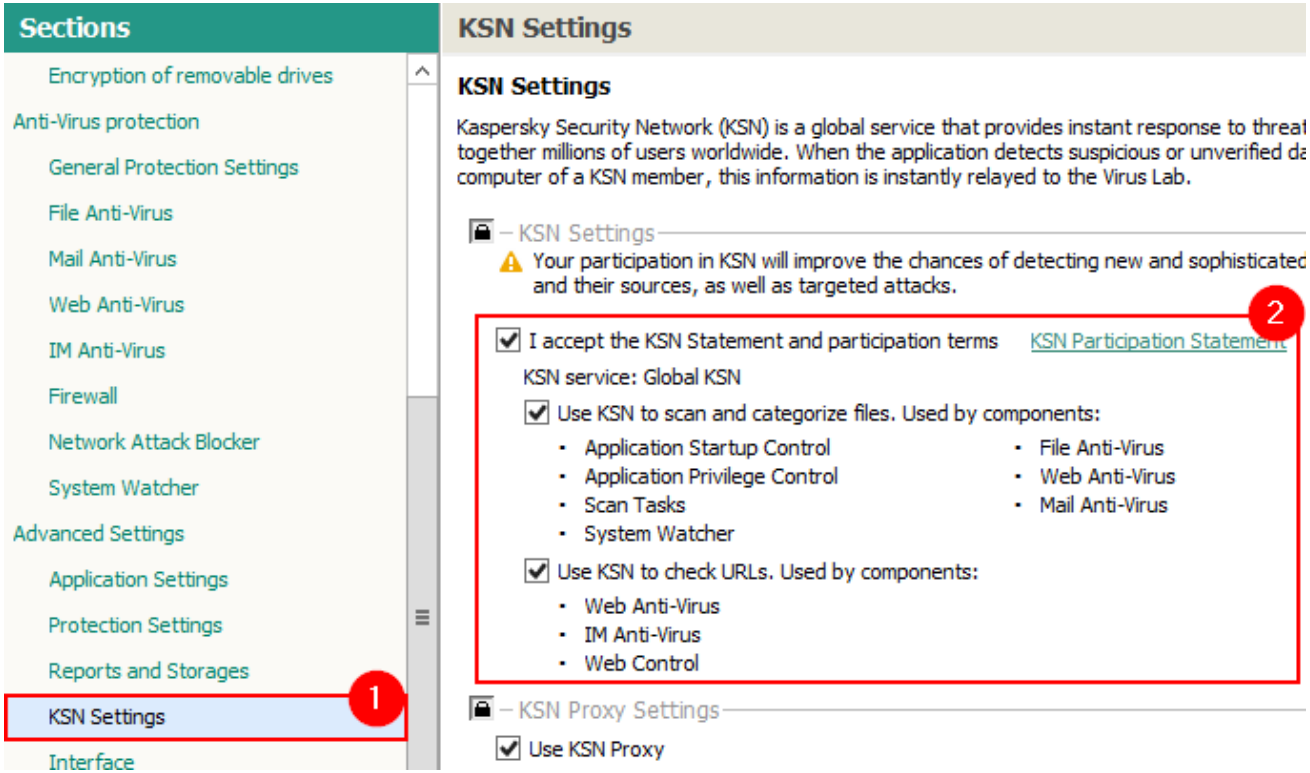
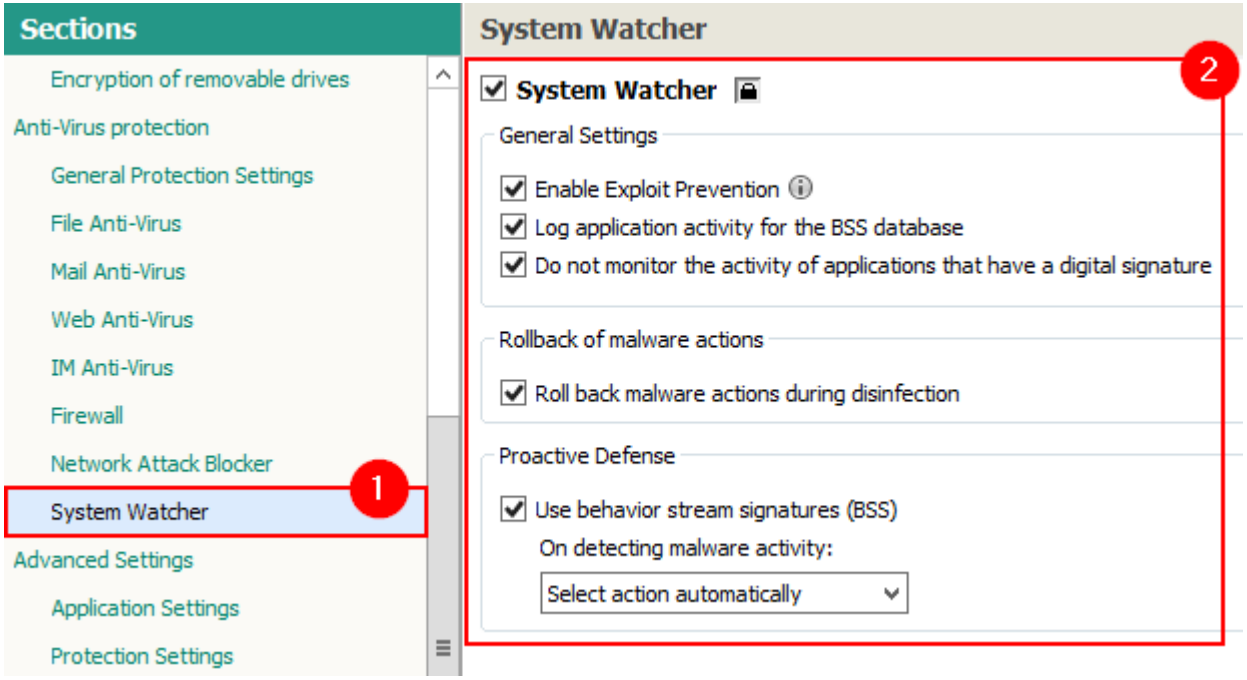
Pasitikrinkite, ar tikrai esate apsaugoti nuo išpirkos reikalaujančių kibernetinių nusikaltėlių!

1. **Patikrinkite ar naudojate naujausią programos versiją -** http://www.kaspersky.com/product-updates
2. **Pagerinkinkite apsaugos modulių nustatymus (pvz.: įjunkite euristiką)**
3. **Įjunkite Kaspersky Security Network**



4. **System Watcher modulis**

   Atidžiai patikrinkite ar System Watcher modulis yra įjungtas nustatymuose Kaspersky Endpoint Security 10 for Windows. Produkto versija Kaspersky Anti-Virus 6 nepalaiko System Watcher modulio! Suinstaliokite naujausia Kaspersky Endpoint Security 10 for Windows versiją. Išsami informacija apie System Watcher modulį rasite čia.



5. **Kaip apsisaugoti nuo „Crypto“ virusų su „Kaspersky Endpoint Security 10 for Windows Workstations“ (darbo vietoms)**

   Tam, kad sumažintumėte „Crypto“ viruso (kenksminga programa, kuri užšifruoja jūsų duomenis ir reikalauja išpirkos) užkrėtimo riziką, rekomenduojame sukonfiguruoti Kaspersky Endpoint Security 10 for Windows nustatymus pagal šią instrukciją. (spauskite nuorodą).

6. **(NAUJIENA) Kaip apsaugoti bendrinamus duomenis tinkle nuo šifruotojų su Kaspersky Security 10 for Windows Servers**

   Anti-Cryptor uždavinys blokuoja nuotolinio ***host'o*** prisijungimą prie serverio, jei buvo užfiksuoti šifravimo bandymai iš šio ***host'o***. Kai nustatomas kenkėjiškas aktyvumas iš nutolusio ***hosto***, Kaspersky Security blokuoja prieigą prie bendrinamų failų tinkle 30 minučių pagal nutylėjimą. Blokavimo laiką galima keisti antivirusinės programos *Untrusted Hosts Blocking* nustatymuose.

7. **Sistemos valdymas**

   Naudokite automatinį pataisų tvarkymą (patch management) iš Kaspersky Endpoint Security for Business – Advanced arba System Management, kad jūsų infrastruktūroje naudojama PĮ būtų nuolat atnaujinama.

8. **Apmokykite savo darbuotojus**

   Isitikinkite, kad kiekvienas darbuotojas išklausytų IT saugumo suvokimo mokymus, tokius kaip on-line arba CyberSafety Games Training iš Kaspersky Security Intelligence Services.

9. **Atsarginis duomenų kopijavimas**

   Naudokite profesionalius sprendimus, sukurtus patikimais gamintojais, kurie turi gilių žinių apie duomenų apsaugą. Atsarginis kopijavimas turi būti pastovus pagal nustatytą tvarkaraštį. Saugokite visas padarytas atsargines kopijas.