



Há muito tempo aprendi que quando não se consegue enxergar explicação, "[siga o link](#)" e ela também registrou no segundo artigo listado.

E então, em fevereiro 2009, depois desses fiascos viabilizados pelo MS-Windows, surge uma matéria ~~Muitas vezes~~ ~~em~~ ~~que~~ ~~ela~~ ~~também~~ ~~registrou~~ ~~no~~ ~~segundo~~ ~~artigo~~ ~~listado~~.  
Muitas vezes as verdades para mascarar mentiras e manter os usuários MS-Windows na **ilusão** de que não existe alternativa e que GNU / Linux não é mais seguro.

Não existe sistema invulnerável.

Você ~~mesmo~~ ~~parte~~ ~~de~~ ~~fazer~~ ambiente desktop GNU / Linux em 5 passos. Não ~~esqueça~~ ~~de~~ ~~parte~~, com algumas propostas de soluções, nem os comentários da primeira parte. Depois, precisa convencer os usuários GNU / Linux a fazer duplo clique no arquivo do seu vírus. O vírus de desktop é possível devido à escolhas default de **alguns** ambientes desktop Linux, nem todos. Mesmo que os estragos sejam limitados por arquitetura (usuários sem privilégios de root) e configurações de muitas distribuições, ainda assim arquivos de um usuários podem ser danificados ou dados vazados.

Mas com GNU / Linux você tem escolhas. Você pode instalar sistemas mínimos e alterar configurações para ainda maior segurança, mesmo sacrificando um pouco da conveniência.

SEMPRE manter seu sistema atualizado usando os repositórios de sua distribuição GNU/Linux. E escolher distribuições que ofereçam suporte sério de segurança para TODO o conteúdo dos repositórios. Ao menos para os que você usa. Nem todas fazem isso porque é trabalhoso e oneroso. Informe-se.

O tempo de amarrar cachorro com linguiça ou de deixar todas as janelas abertas já acabou há muito tempo.

Com um pouco de informação, o usuário de GNU/Linux continua muito mais seguro que um usuário de sistemas Microsoft.

E mesmo sem informação, ainda fica mais seguro que usando MS-Windows, usando

distribuições renomadas e seguras como Debian GNU/Linux.

Informação vai proteger seu dinheiro e seu negócio.