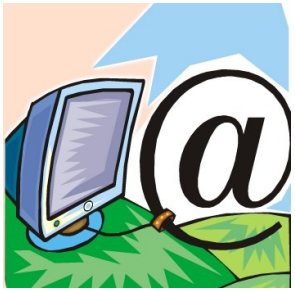
Segurança no Computador



Para aumentar a segurança no computador pessoal, basta seguir alguns conselhos simples e práticos, que protegem o computador dos problemas mais comuns, tais como:

1. Garanta que o sistema operativo e os programas instalados apresentam as actualizações mais recentes. Tal como um carro, o computador também necessita de manutenção. Por isso actualize, com frequência, o sistema operativo e todos os programas.

2. Certifique-se que tem um anti-vírus e um "anti-spyware" instalados, bem como uma "firewall" activada. Mantenha-os a todos devidamente actualizados.

3. Use uma conta de utilizador, sem direitos de administração, no dia-a-dia, quando trabalha com o seu computador; guarde a conta de administração somente para quando pretende instalar programas ou alterar configurações no computador.

4. Faça cópias de segurança com a regularidade que entenda mais apropriada, de acordo com a importância que atribui aos documentos e ficheiros que produz e armazena no seu computador. Para tal pode usar uma "pen drive", um CD ou DVD, um disco externo ou, ainda, um servidor on-line.

REFERÊNCIA BIBLIOGRÁFICA

SeguraNet - *Segurança no computador*. [Em linha]. [Consult.17 de Janeiro de 2011]. Disponível em: WWW:<URL: http://www.seguranet.pt/educadores/>.

ESCOLA SECUNDÁRIA DR. JOAQUIM DE CARVALHO, FIGUEIRA DA FOZ

BIBLIOTECA ESCOLAR

BLOGUE: http://www.netbiblio.blogspot.com

E-mail: biblioteca@esjcff.pt

Escola Secundária Dr. Joaquim de Carvalho, Figueira da Foz
Biblioteca Escolar

Guia

SeguraNet

Segurança no Computador

Segurança no Computador

O que é um vírus informático?

Um vírus informático ou vírus de computador é um programa informático que tem como propósito "infectar" o computador, fazendo com que o seu sistema operativo fique corrompido. O vírus ataca agregando-se a um determinado programa, já instalado no computador, de forma a que, quando este arranca, o vírus arranca com ele, propagando uma "infecção". Este fenómeno ocorre, normalmente, sem o conhecimento do utilizador. Ao "infectar" o sistema operativo, um vírus poderá replicar-se a si mesmo e tentar "infectar" outros computadores, através de diversos meios.

Um vírus tanto pode ser um inofensivo programa que pouco mais faz que incomodar ligeiramente, como pode ir ao extremo de destruir ficheiros e tornar um computador inoperável. Contudo, uma característica comum a todos os vírus é a velocidade com que se propagam, contaminando outros ficheiros e computadores, ligados à Internet, que se revelem mais vulneráveis.

Como funcionam os vírus?

Uma das formas mais comuns de transmissão de vírus é através do e-mail. Há programas virais que se propagam de máquina em máquina através do uso das moradas de e-mail que figuram na lista do "utilizador infectado". Outro método usado é pelo envio de uma mensagem de e-mail que, por exemplo, prometa prémios caso o utilizador descarregue o ficheiro que se encontra nessa mensagem. Outras formas de infecção podem incluir o download acidental de programas maliciosos que se encontrem "escondidos" dentro de outros programas, ou clicando em determinadas áreas de certos sítios de Internet mal intencionados.
A segunda maior causa de infecção deve-se ao facto de o utilizador não manter o seu sistema operativo actualizado, com a instalação dos "patches" ("remendos") que o fabricante vai disponibilizando, à medida que vai detectando falhas.

Apresentamos, de seguida, algumas técnicas de "auto-preservação" dos vírus:

•Ocultação, nas pastas do sistema

Dado que uma grande parte dos utilizadores de computadores não possui conhecimentos especializados em informática, os vírus implantam-se no sistema operativo, a fim de evitar que o utilizador comum tente removê-los. Esta técnica acaba por ser dissuasora, porque o utilizador médio terá receio de remover ficheiros do sistema, corrompendo o normal funcionamento do seu sistema.

•Encriptação

Os vírus "escondem-se" encriptando os seus próprios dados: assim, o seu código será mais dificilmente detectado pelos antivírus e será mais difícil a sua remoção, embora cada vez mais os antivírus estejam melhor preparados para esta técnica. O propósito desta técnica é manter a infecção o maior tempo possível, no computador.

•Tentativas de desactivar o antivírus

Esta é a melhor forma de o vírus evitar a sua detecção e remoção.

Que perigos podem apresentar os vírus?

Um vírus de computador está programado para se esconder da melhor forma possível, para evitar a sua detecção e remoção.

Uma infecção por vírus pode trazer sérias consequências para o proprietário do material infectado pois corrompe ficheiros, podendo até inutilizá-los, torna o sistema operativo muito mais lento e, por vezes, pode até usurpar os dados pessoais do utilizador.

Para saber mais acerca dos malefícios dos vírus, consulte as secções e-mail e phishing.

Que cuidados ter?

•Tenha o antivírus actualizado

Embora não seja infalível, um antivírus ajuda-o a evitar que muitos vírus infectem o seu computador.

•Não abra ficheiros de origem suspeita

Os ficheiros enviados por e-mail, mesmo de origem conhecida, podem conter material malicioso. Corra-os primeiro com o antivírus. Se forem de origem desconhecida ou se desconfiar de phishing, não abra esses ficheiros.

•Tenha o seu sistema operativo actualizado

O fornecedor do sistema operativo actualizará, de forma gratuita, no seu sítio de Internet, os chamados "patches" ("remendos") para corrigir eventuais fragilidades que possam facilitar a entrada de programas maliciosos. Tenha sempre o seu computador actualizado.

•Tenha a firewall sempre activa

Uma firewall é uma protecção adicional contra a entrada de programas indesejados no seu computador, pelo