A correcta utilização do correio electrónico

O correio electrónico, é um dos meios de comunicação mais utilizados, hoje em dia, seja para enviar uma mensagem de amizade, uma informação, ou um trabalho, etc. Porém, através do correio electrónico podemos contaminar nosso computador com a propagação de vírus cada vez mais poderosos. Para evitar problemas e prevenir contra a infecção de nossos computadores, é importante seguirmos algumas sugestões:

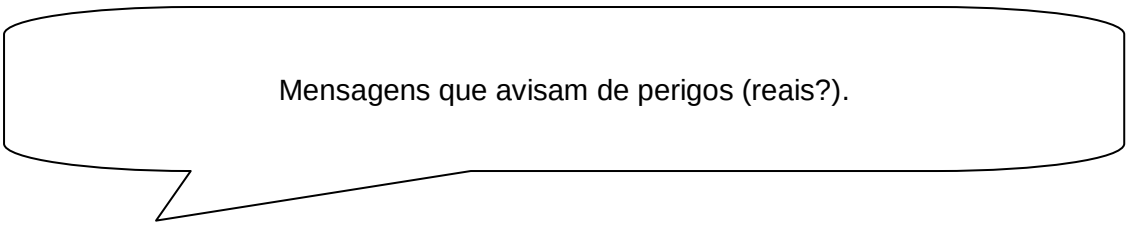
Corra uma aplicação antivírus e mantenha-a actualizada.

Ter um software antivírus sempre activado e actualizado ajuda a prevenir que as mensagens de conteúdo malicioso consigam infectar o sistema. Use sempre o antivírus para examinar as mensagens e anexos que lhe forem enviados. Muitos pacotes antivírus suportam actualização automática de definições de vírus. A utilização destas actualizações automáticas é recomendável.

Tenha o filtro anti-SPAM activado nas configurações do servidor de e-mail

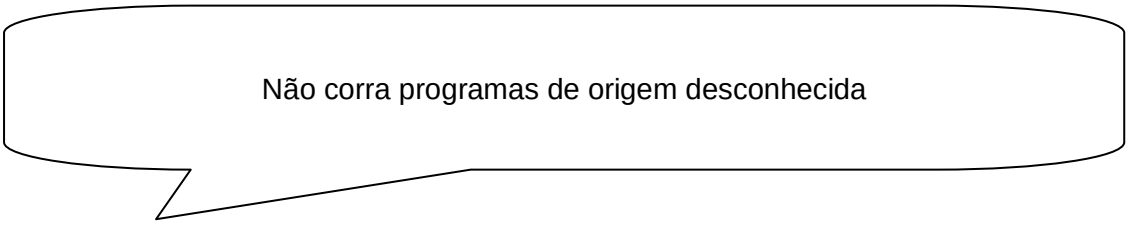
A maioria dos servidores de correio electrónico possui a funcionalidade de filtragem de SPAM. Embora não seja infalível, esta faz com que muitos dos e-mails, de origem considerada suspeita, sejam enviados directamente para uma pasta própria. Verifique esta pasta com frequência, dado que poderá dar-se o caso de alguma mensagem legítima ser para ali encaminhada, por engano.

Desconfie de mensagens de entidades que o informam que ganhou prémios.



O utilizador pode receber, na sua caixa de correio electrónico, mensagens de alarme acerca de vírus, fenómenos alarmantes ou perigos para a saúde, entre outros, contendo informação que, à primeira vista, parece verdadeira, mas, muitas vezes, não é. A estes e-mails dá-se o nome de "Hoaxes" ou embustes, e o seu propósito é impelir o utilizador a reenviar aquela mensagem para o maior número de pessoas conhecidas e, assim, apropriarem-se de moradas de e-mail que, depois, enchem de SPAM.

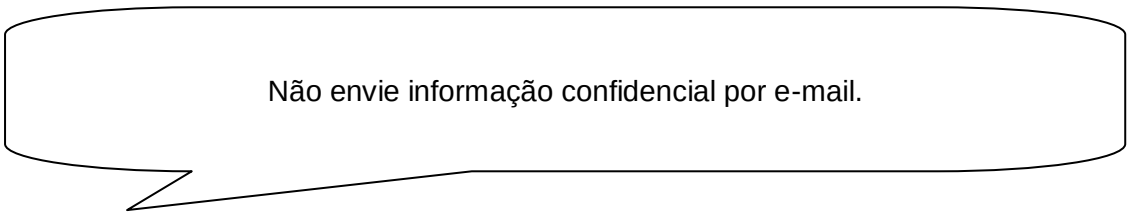
Consulte sempre fontes de segurança legítimas (como o seu servidor de antivírus) a fim de se certificar que o conteúdo deste tipo de mensagens é legítimo, antes de as enviar aos seus contactos.



Desligue as opções que permitem abrir ou executar automaticamente ficheiros ou programas anexados às mensagens.

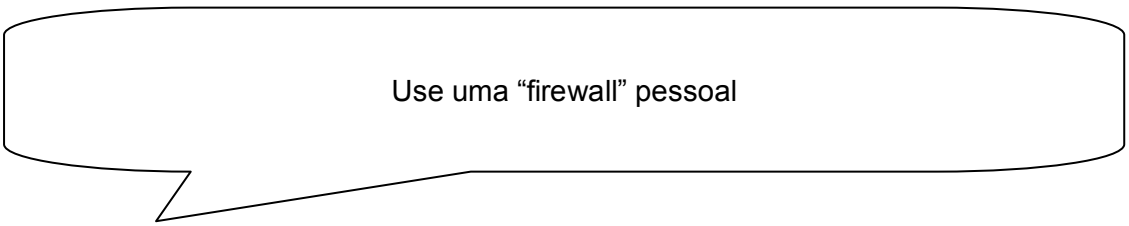
Não descarregue, nem instale ou corra programas a menos que saiba que são da autoria de pessoas ou companhias em que confia. Os utilizadores de e-mail devem suspeitar de anexos inesperados. Certifique-se de que conhece a origem de um anexo, antes de o abrir. Lembre-se, também, que não basta que a mensagem tenha origem num endereço que reconhece, dado que os computadores dos seus contactos podem estar infectados.

Os utilizadores devem ainda acautelar-se contra URLs (Uniform Resource Locator, isto é, o endereço de um recurso, que poderá estar sob a forma de link na mensagem) nas mensagens de correio electrónico. Os URLs podem conduzir a conteúdo malicioso que, em certos casos, poderá ser executado sem intervenção do utilizador. Um exemplo disto é o phishing, que utiliza URLs enganadores para levar os utilizadores a visitar “web sites” maliciosos.



O correio electrónico não é um meio seguro para enviar informação ou dados que não deseja que sejam vistos por terceiros, dado que podem ser interceptados, no seu percurso.

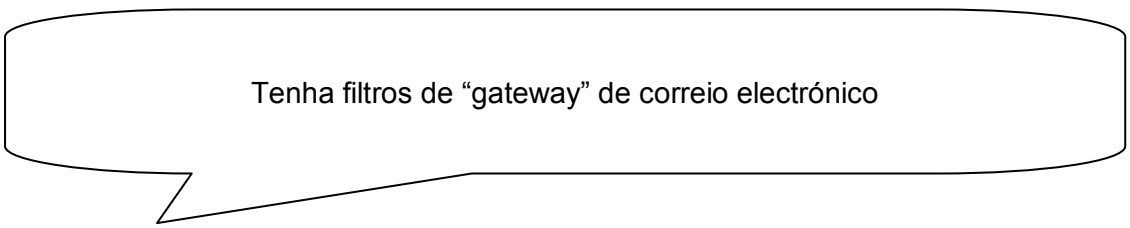
Se desejar enviar informação confidencial, recorra a e-mails cifrados. Existem várias soluções comerciais ou gratuitas (“freeware”) ao seu dispor, na Internet, que codificam os seus dados, do remetente para o receptor.



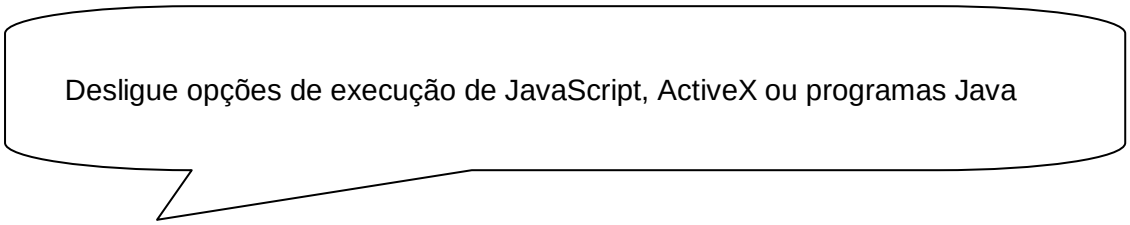
As “firewalls” filtram portos e protocolos desnecessários, de Internet, evitando que o utilizador corra programas ou páginas de Internet potencialmente prejudiciais.

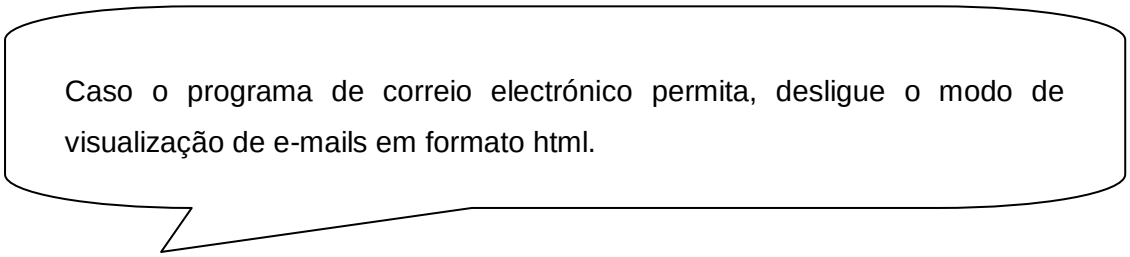
Uma “firewall” pessoal não protegerá, necessariamente, o seu sistema, de um vírus propagado por correio electrónico, mas uma devidamente configurada pode evitar que o vírus descarregue componentes adicionais ou lance ataques contra outros sistemas.

Infelizmente, uma vez dentro do sistema, um vírus pode activar ou desactivar uma “firewall” de “software”, eliminando assim a sua protecção.



Dependendo das necessidades do seu negócio, é recomendável a configuração de filtros no “gateway” contra ficheiros com extensões específicas nos anexos de mensagens de e-mail. Esta filtragem deve ser configurada com cuidado, já que poderá afectar, também, anexos legítimos. Recomenda-se que os anexos fiquem em “quarentena” para posterior exame e/ou possível recuperação.





Referência:
SeguraNet http://www.seguranet.pt/educadores/ pesquisado no dia 02/01/11
Adaptado por Carla Barbosa.