O que é o E-mail?

O e-mail (abreviatura de “electronic mail”, ou correio eletrónico, em português) consiste num meio de enviar mensagens escritas, pela Internet, com a vantagem de serem recebidas quase instantaneamente pelo destinatário, em qualquer parte do mundo onde haja ligação de Internet, dispensando intermediários, selos e a espera dos correios tradicionais.

Outra grande funcionalidade deste meio traduz-se na possibilidade de o utilizador criar listas de distribuição de endereços de correio eletrónico, podendo enviar uma mensagem para várias pessoas, ao mesmo tempo.

Como funciona o correio electrónico?

Para se enviar um e-mail, basta ao utilizador:

• possuir uma ligação à Internet;

• estar registado num servidor de e-mails;

• escrever a sua mensagem, colocando o endereço eletrónico do destinatário no local apropriado e;

• proceder ao seu envio, clicando na área apropriada desse mesmo servidor.

No entanto, tal como para outras funcionalidades da Internet, também o correio eletrónico tem os seus perigos, como a propagação de vírus, devendo o utilizador tomar algumas precauções para assegurar, ao máximo, a proteção dos seus dados e do seu computador.

REFERÊNCIA BIBLIOGRÁFICA

SeguraNet - *A correcta utilização do correio electrónico*. [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

Correio Electrónico

Correio Electrónico

Que perigos pode apresentar uma mensagem de correio eletrónico?

Um dos perigos mais comuns do correio eletrónico é a propagação de vírus e consequente infeção dos computadores de utilizadores domésticos e empresariais.
Os vírus são propagados de diversas formas, como por exemplo, através de mensagens não solicitadas de correio eletrónico contendo anexos, que são enviados para os mais diversos destinatários. Estes e-mails podem conter endereço de retorno, um envelope provocante ou qualquer outro artifício que encoraje o recetor a abri-lo.
A este tipo de técnica de encorajamento dá-se o nome de Engenharia Social (sendo disto um grande exemplo o Phishing).

Uma infeção por vírus pode ter consequências nefastas no seu sistema informático como, por exemplo:

• Revelar informação
Os vírus propagados por mensagens de correio eletrónico em massa (SPAM) podem ter como principal objetivo a recolha de endereços de correio eletrónico da lista de contactos do utilizador ou de ficheiros.

Alguns vírus também tentarão enviar ficheiros de uma máquina infectada para outras potenciais vítimas ou até para o autor do vírus. Estes ficheiros podem conter informação sensível.

• Instalar uma "backdoor"
Uma "backdoor" ("porta de fundos", em português) pode ser usada por um atacante remoto para conseguir acesso ao sistema, ou para adicionar/modificar/apagar ficheiros, no sistema. Estas "backdoors" podem também ser manipuladas para descarregar e controlar ferramentas adicionais para uso em ataques distribuídos de negação de serviços (Distributed Denial of Service – DDoS) contra outros sítios de Internet.

• Atacar outros sistemas
Os sistemas infestados por vírus são frequentemente utilizados para atacar outros sistemas. Estes ataques envolvem, muitas vezes, tentativas de explorar vulnerabilidades do sistema remoto ou ataques de negação de serviços que consomem grandes volumes de tráfego na rede.

• Atacar outros sistemas
Os sistemas infestados por vírus são frequentemente utilizados para atacar outros sistemas. Estes ataques envolvem, muitas vezes, tentativas de explorar vulnerabilidades do sistema remoto ou ataques de negação de serviços que consomem grandes volumes de tráfego na rede.

• Enviar correio eletrónico não solicitado em massa (SPAM) a outros utilizadores
Há inúmeras participações de "spammers" utilizando sistemas comprometidos para enviar e-mails em massa. Estes sistemas comprometidos são, com frequência, computadores mal protegidos para utilização "final" (ex.: sistemas domésticos e de pequenas empresas).

Que cuidados ter?

Uma utilização informada continua a ser a melhor forma de prevenir a infeção do seu computador. Aqui se apresentam algumas sugestões de prevenção.

• 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.

Os fabricantes dos softwares antivírus publicam, frequentemente, informação atualizada, ferramentas ou bases de dados de vírus para ajudar na deteção e recuperação de código malicioso. Muitos pacotes antivírus suportam atualização automática de definições de vírus. A utilização destas atualizações automáticas é recomendável.

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

A maioria dos servidores de correio eletrónico 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 diretamente 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.

• Mensagens que avisam de perigos (reais?)

O utilizador pode receber, na sua caixa de correio eletrónico, 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.

• Não corra programas de origem desconhecida

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. Suspeite 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.

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

• Não envie informação confidencial por e-mail

O correio eletrónico não é um meio seguro para enviar informação ou dados que não deseja que sejam vistos por terceiros, dado que podem ser intercetados, 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 recetor.

• Use uma "firewall" pessoal

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 eletrónico, 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 ativar ou desativar uma "firewall" de "software", eliminando assim a sua protecção.

• Tenha filtros de "gateway" de correio electrónico

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 afetar, também, anexos legítimos. Recomenda-se que os anexos fiquem em "quarentena" para posterior exame e/ou possível recuperação.

• Desligue opções de execução de JavaScript, ActiveX ou programas Java

• Caso o programa de correio eletrónico permita, desligue o modo de visualização de e-mails em formato html.