

Segurança na Internet e Intranet

Etapas essenciais para atingir alguma segurança

Bom Senso	Não há nenhum programa que nos proteja a 100% se não tomarmos algumas precauções. Por ex. Nunca abrir ficheiros vindos de desconhecidos (por email, chat ou outros), não deixar o nosso computador desprotegido, etc.
AntiVírus	Utilizado para detectar e eliminar vírus. Tem de ser actualizado regularmente, de forma a reconhecer os vírus, worms e cavalos de tróia mais recentes. Exemplos: Avast! : http://www.avast.com AVG : http://www.grisoft.com Norton : http://www.symantec.com Panda : http://www.pandasoftware.com Mcafee : http://www.mcafee.com
Firewall	Utilizada para determinar que programas podem aceder à internet, e impedir que intrusos entrem no nosso PC. Pode ser visto como uma espécie de guarda ou porteiro, pois decide quem pode entrar e quem pode sair. Exemplos: ZoneAlarm : http://www.zonealarm.com Norton : http://www.symantec.com Panda : http://www.pandasoftware.com Mcafee : http://www.mcafee.com
Actualizar Software	Sempre que falhas (bugs) e outras vulnerabilidades são encontradas, o criador do software geralmente disponibiliza correcções (patches), ou até mesmo novas versões. É importante manter o nosso software actualizado. Exemplos: Actualizações da Microsoft: http://windowsupdate.microsoft.com Linux – Caixa Mágica: http://www.caixamagica.pt Linux – Mandrake: http://www.mandriva.com Browser Mozilla FireFox: http://www.mozilla.com
Cópias / Backup	Não há segurança total, pelo que devemos estar prevenidos e termos cópias de segurança dos nossos dados mais importantes (CD/DVD, Pen Drive, etc).

Perigos na Internet, formas de propagação e precaução

Vírus	<p>Objectivo: danificar o computador do utilizador, ou roubar informação.</p> <p>Método de propagação: via email (como anexo), disquetes, CD-ROM's, entre outros, e multiplica-se infectando outros programas ou ficheiros.</p> <p>Solução: Não abrir ficheiros de origem ou função desconhecida. Instalar e actualizar regularmente o antivírus.</p>
Worms	<p>Objectivo: atacar o computador de determinadas entidades / empresas, mas durante esse processo pode danificar o nosso PC, ou roubar informação.</p> <p>Método de propagação: pela Internet ou outra rede, enviando cópias de si mesmo de PC para PC, através da exploração de vulnerabilidades / falhas.</p> <p>Solução: Instalar e configurar firewall. Instalar e actualizar regularmente o antivírus. Actualizar Sistema Operativo e outras aplicações.</p>
Cavalos de Tróia	<p>Objectivo: obter acesso ao computador do utilizador, de forma a ler e roubar informação, alterar ou destruir ficheiros, isto é, controlar todo o sistema.</p> <p>Método de propagação: necessita ser instalado manualmente, pelo que geralmente vem disfarçado de jogo, protecção de ecrã, ou outra aplicação.</p> <p>Solução: Não abrir ficheiros de origem ou função desconhecida. Instalar e configurar firewall. Instalar e actualizar regularmente o antivírus.</p>
Fraude	<p>Objectivo: obter senhas de acesso (da conta bancária, do ISP, do email, entre outros), quantias em dinheiro, ou instalação de cavalos de tróia.</p> <p>Método de propagação: envio de email, chamada telefónica, ou chat.</p> <p>Solução: Não acreditar em tudo o que se lê ou ouve.</p>
Spyware e Dialers	<p>Objectivo: instalar formas abusivas de publicidade (spyware) e programas que efectuem chamadas telefónicas de valor acrescentado (dialers).</p> <p>Método de propagação: necessita ser instalado manualmente, ou via Internet, pelo aparecimento de janela que pede para instalar um programa.</p> <p>Solução: Em caso de dúvida, entre "OK" e "Cancelar", clicar em "Cancelar". Eliminar Spyware com um programa chamado LavaSoft AdAware: http://www.lavasoftusa.com/software/adaware</p>

Recomendações

Actualizações frequentes:

- Actualizar regularmente o antivírus, sistema operativo e todos os outros programas, de forma a não estar vulnerável aos riscos mais recentes, inclusive ataques de hackers.

Cuidados a ter com o email e chat:

- Nunca abrir ficheiros anexos (documentos, programas ou imagens) de origem ou função desconhecida. Ficheiros aparentemente inofensivos podem estar camuflados. Em último caso deveremos verificá-los com um antivírus actualizado, pois existem vírus que se reenviam a partir dos emails dos nossos amigos (e chegam até nós com o seu endereço).

- Não acreditar em todos os boatos e fraudes que circulam na Internet. Ninguém consegue doar ou receber dinheiro por enviar emails, seja qual for a razão.

- Nunca enviar dados importantes num email ou chat. É costume tentar descobrir passwords / senhas de acesso desta forma.

- Para sairmos do site onde consultamos o nosso email / correio electrónico, não basta fechar a janela. Devemos carregar no botão Sair ou Logout.

Cuidados a ter com os downloads:

- Sempre que efectuar algum download, deveremos verificá-lo com o antivírus. E mesmo verificando nunca se deverá confiar em demasia, pois um antivírus pode não reconhecer um vírus mais recente. Há também que ter cuidado com aplicações chamadas keyloggers, que registam tudo o que escrevemos, e nem sempre são detectadas.

Cuidados a ter com as senhas de acesso / passwords:

- Escolher uma senha / password que não seja fácil de adivinhar. Nunca usar datas de nascimento, siglas do próprio nome, nomes de pessoas importantes para nós, ou palavras comuns do dicionário. O ideal será utilizar um conjunto de letras e números (se recorrermos a maiúsculas e minúsculas será ainda mais difícil de descobrir).

Exemplo: Sala5Tic8

- Nunca usar a mesma palavra chave, e deveremos alterá-la frequentemente.

Cuidados a ter com os nossos dados pessoais:

- Nunca fornecer o nosso nome, morada ou número de telefone, sem termos a certeza de que será seguro fazê-lo. A privacidade de dados pessoais é fundamental.