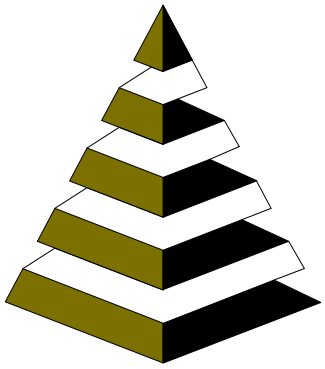
Segurança Informática para Todos



FUNDAÇÃO para a *DIVULGAÇÃO*
das *TECNOLOGIAS* de *INFORMAÇÃO*

Título: Segurança Informática para Todos
Autor: Carlos Alberto Marques Brás
Capa: Rodrigo Monteiro Baptista

Impressão e acabamento: Tipografia
Depósito Legal n.º xxxxx/05

A **Fundação para a Divulgação das Tecnologias de Informação** (FDTI), instituída pelo Instituto Português da Juventude e pelo Instituto do Emprego e Formação Profissional, tem como fim promover a divulgação das Tecnologias de Informação de forma extensiva e sistemática, junto dos jovens e junto das comunidades.

A **FDTI**, de forma a alcançar os seus objectivos, conta com uma rede nacional de Centros de Divulgação das Tecnologias da Informação (cerca de 170), geograficamente distribuídos por todos os Distritos do território continental e pelas Regiões Autónomas dos Açores e da Madeira.

Nestes centros proporciona-se formação, estruturada em módulos, que permite a iniciação ou o aperfeiçoamento de conhecimentos na área das Tecnologias de Informação.

A qualidade dos produtos e serviços que desenvolve, entre os quais se incluem os manuais da linha editorial, assume enorme importância para a FDTI.

É nosso objectivo que o presente manual constitua um bom auxiliar de aprendizagem, e que com ele, a FDTI continue a prestar à Sociedade Portuguesa um serviço de qualidade.

Esta brochura faz parte da linha editorial da responsabilidade da FDTI - Fundação para a Divulgação das Tecnologias de Informação.

No final desta brochura encontrará a lista dos cursos que compõem a oferta formativa da FDTI bem como os títulos editados por esta Linha Editorial.

Para obter informação mais completa sobre os cursos e os manuais da FDTI, ou para aceder às erratas dos manuais, visite o sítio:

http://fdti.juventude.gov.pt

Se pretender emitir observações, sugestões ou críticas sobre a Linha Editorial, em geral, ou sobre esta obra, em particular, envie, por favor, uma mensagem para o endereço de correio electrónico:

linhaeditorial@fdti.pt

Índice

capítulo 1

Introdução

- **Introdução**
- **Porquê preocupar-se com a segurança?**

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

Introdução

As TIC (Tecnologias de Informação e Comunicação) têm vindo a mudar radicalmente a vida das pessoas. Nos dias que correm quase tudo está informatizado e, a cada dia que passa, aparecem novas tecnologias em substituição das actuais a uma velocidade estonteante.

Apesar das TIC facilitarem a vida aos seus utilizadores, nem tudo é um "mar de rosas".

Para além de todos os benefícios e comodidades que resultam da utilização das TIC, também é de salientar os riscos e problemas de segurança que daí advêm.

Com a massificação da utilização das TIC nas mais diversas finalidades, torna-se por demais evidente, mais do que uma necessidade, uma obrigatoriedade, a implementação de formas e métodos de protecção e segurança da informação quer pessoal quer institucional.

Esta brochura dirige-se, essencialmente, ao utilizador doméstico e tem como objectivos alertar e elucidar para os perigos existentes na utilização diária do computador, bem como deixar algumas medidas por forma a aumentar a segurança na utilização do computador pessoal e diminuir o risco de perda de informação ou transmissão de dados pessoais.

Esta brochura foi escrita a pensar nos utilizadores do Windows XP, no entanto, a maioria dos temas aqui tratados é válida para a generalidade dos sistemas operativos.

Porquê preocupar-se com a segurança?

Os computadores pessoais, hoje em dia, são utilizados para realizar as mais diversas tarefas, tais como:

- Transacções financeiras, quer sejam bancárias ou mesmo através da compra de bens ou serviços;
- Comunicação, por exemplo através de mensagens de correio electrónico;
- Armazenamento de informação, quer pessoal quer profissional, etc.;

Desta forma, torna-se importante a preocupação com a segurança do computador, pois, provavelmente ninguém gostaria que lhe acontecesse alguma das seguintes situações:

- Palavras-passe (*passwords*) e números de cartões de crédito furtados e utilizados por estranhos;
- Utilização da conta de acesso à Internet por terceiros, não autorizados;
- Dados pessoais ou profissionais alterados, destruídos ou visualizados por estranhos, etc..

capítulo 2

3 passos para proteger o PC

- **1º Passo: utilizar *firewall***
- **2º Passo: actualizar o computador**
- **3º Passo: utilizar *software* antivírus actualizado**

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

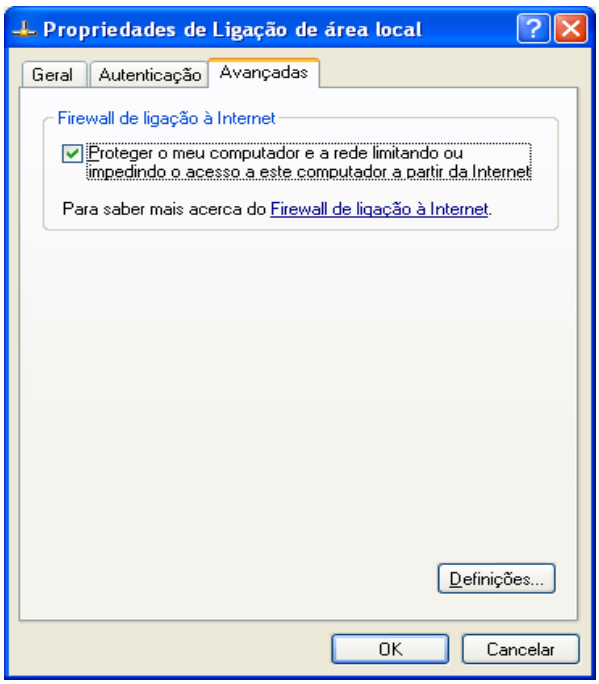
Proteger o PC

Seguir apenas três passos, simples e básicos, é uma das formas que permite aumentar a segurança do computador pessoal evitando, desta forma, alguns dos problemas comuns ao utilizador doméstico.

1º Passo: utilizar *firewall*

No seu conceito básico, uma *firewall* tem como função impedir a estranhos o acesso ao computador através da Internet.

Uma *firewall* tanto pode ser física (*hardware*), como um simples programa (*software*) que implementa um determinado conjunto de regras por forma a impedir/bloquear determinados acessos maliciosos ao computador, nomeadamente bloqueando grande parte dos *Trojans* (cavalos de Tróia), mesmo que estes já se encontrem instalados no computador.



Para activar a *firewall* do Windows XP aceda às propriedades da ligação de rede, a partir do **Painel de controlo**. No separador **Avançadas** active a opção **Proteger o meu computador e a rede limitando ou impedindo o acesso a este computador a partir da Internet**.

2º Passo: actualizar o computador

Um dos passos importantes para o aumento da segurança consiste em manter sempre o seu sistema operativo, e demais programas instalados no computador, a funcionar com as últimas actualizações disponíveis.

Quando um *software* é lançado no mercado, é comum que surjam algumas "brechas" de segurança. Para que estas brechas não tragam problemas ao utilizador, normalmente as entidades responsáveis por esse *software* lançam actualizações que permitem eliminar esses problemas, aumentando desta forma a segurança do computador.

3º Passo: utilizar *software* antivírus actualizado

Os antivírus são programas que permitem detectar, anular e eliminar os vírus informáticos.

Actualmente os programas antivírus têm vindo a adquirir novas funcionalidades, permitindo também eliminar *trojans*, barrar programas *Java* e *ActiveX* nocivos ao computador, bem como efectuar uma verificação às mensagens de correio electrónico.

É de vital importância que o *software* antivírus esteja permanentemente actualizado, pois estão sempre a surgir vírus que podem representar novas ameaças para o computador e a informação nele guardada.

capítulo 3

Problemas de segurança

- **Introdução aos problemas de segurança**
- ***Phishing* - engenharia social**
- ***Trojans* - cavalos de Tróia**
- **Vírus**
- ***Worms***
- ***Spyware***
- ***Cookies***
- ***SPAM***
- ***Hoaxes* - boatos**

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

Introdução aos problemas de segurança

Existem diversas formas e métodos de perturbar a segurança dos sistemas. Neste capítulo são apresentados alguns dos mais conhecidos problemas de segurança com que se depara um utilizador, tais como vírus, *trojans*, *worms*, etc.

Phishing - engenharia social

O termo engenharia social é empregue para designar métodos de obtenção de informações importantes relativas ao utilizador, através da sua confiança ou ingenuidade.

Normalmente, estes métodos estão relacionados com o envio de mensagens de correio electrónico a solicitar dados pessoais, dizendo tratar-se de uma campanha do banco ou do ISP (*Internet Service Provider*), ou referenciando a possibilidade de receber uma herança, entre outros assuntos possíveis. Para que o utilizador possa beneficiar do que lhe é prometido na mensagem, são-lhe solicitados alguns dados pessoais, como o nome de utilizador, palavra-passe, ou mesmo dados referentes a cartões de crédito.

Outra das aparências possíveis de uma mensagem de correio electrónico utilizada por estes métodos consiste na solicitação da contribuição do utilizador para uma determinada causa.

Para que o utilizador não corra o risco de disponibilizar os seus dados a estranhos, mal intencionados, não deve confiar neste tipo de mensagens.

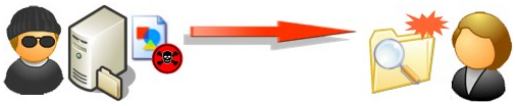
É importante referir que este método não é só empregue através da utilização do correio electrónico, mas também pode ocorrer por telefone ou através de fóruns ou programas de mensagens instantâneas.

Trojans - cavalos de Tróia

O termo cavalo de Tróia (*trojan*) vem da mitologia grega, em que os gregos para conseguirem conquistar a cidade de Tróia, muito fortificada, construíram um enorme cavalo em madeira e ofereceram-no aos troianos. Dentro do cavalo estavam centenas de soldados gregos que, durante a noite, abriram os portões da cidade de Tróia, permitindo assim a conquista desta cidade por parte dos gregos. Deste acontecimento surgiu a expressão "cavalo de Tróia".

Nos nossos dias, a expressão cavalo de Tróia ou *trojan*, é utilizado, em informática, para identificar alguns programas que se instalam no computador, muitas vezes sem que o utilizador se dê conta da sua ocorrência.

Os *trojans* podem vir como anexo de uma mensagem de correio electrónico ou junto com *software* pirata retirado da Internet, por exemplo.

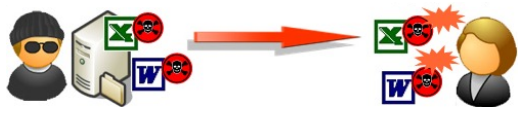


Os *trojans*, uma vez instalados num computador, têm como principal finalidade abrir algumas portas por forma a permitir o roubo de informação pessoal, tal como palavras-passe, ficheiros, etc..

Vírus

Um vírus é um trecho de código de programa que se anexa a um ficheiro ou programa, por forma a propagar-se de computador em computador.

Os vírus existem sob variadas formas e com diversos níveis de importância de danos causados, que vão desde fazer aparecer um inocente boneco no ecrã até danificar o computador (incluindo o *hardware*).



Normalmente, os vírus não se propagam sem que exista uma intervenção do utilizador, ou seja, são propagados através da troca de disquetes usadas em computadores infectados, de mensagens de correio electrónico, etc..

Worms

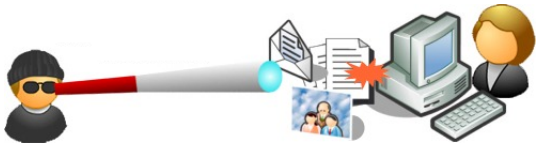
Um *worm*, apesar de ter a mesma finalidade de um vírus, possui a capacidade de se propagar automaticamente, ou seja possuem a capacidade de se replicarem em grandes quantidades.

Por exemplo, um *worm* pode enviar cópias de si próprio para todas as pessoas que estejam no livro de endereços de um computador infectado com o *worm*.

Os *worms* são, no fundo, uma subclasse de vírus, que têm como finalidade uma rápida propagação pela rede, consumindo recursos da rede e dos computadores nela ligados (memória, largura de banda, etc.).

Spyware

O *spyware* é um tipo de *software* malicioso que pode vir integrado noutros programas ou em determinados componentes *web* que são transferidos ao aceder a uma página de Internet.



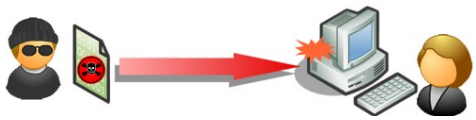
Denota-se a existência de *spyware* num computador através de um ou vários dos seguintes sintomas:

- **O *browser* abre-se sozinho, apresentando determinados anúncios;**
- **A página principal do *browser* é alterada inadvertidamente, sem que o utilizador o tenha efectuado;**
- **São adicionadas páginas *web* aos Favoritos sem que o utilizador o faça;**
- **Aparecimento de novas barras de ferramentas no *browser*;**
- **O *browser* fecha-se e deixa de responder;**
- **O utilizador deixa de conseguir iniciar determinados programas.**

Grande parte do *spyware* pode ser desinstalado normalmente do computador, no entanto, existem alguns que são um pouco mais difíceis de retirar do computador. Para limpar completamente o computador de *spyware* que esteja instalado, existem algumas ferramentas disponíveis na *web* para o efeito.

Cookies

Os *cookies* são pequenas informações guardadas, pelos *sites* visitados pelo utilizador, no *browser*.



Os *cookies* podem ser utilizados de diversas formas:

- **Guardar a identificação do utilizador enquanto este navega entre as páginas do mesmo *site*;**
- **Manter uma "lista de compras" em *sites* de comércio electrónico;**
- **Personalizar *sites* pessoais ou de notícias, quando o utilizador escolhe o que deseja ver, e como o deseja, nestes *sites*;**
- **Manter alvos de *marketing*, quando se visita um *site* e se procura uma determinada informação, na próxima visita ao *site* aparecerá logo essa informação sob a forma de publicidade, etc..**

Em alguns dos casos os *cookies* são benéficos para o utilizador, o problema coloca-se quando estes são utilizados por entidades que vasculham as preferências do utilizador e espalham essa informação para outros *sites*. Este tipo de situação nota-se quando, ao navegar na Internet, surgem, de forma autónoma, anúncios e publicidade a produtos sobre os quais o utilizador havia pesquisado recentemente.

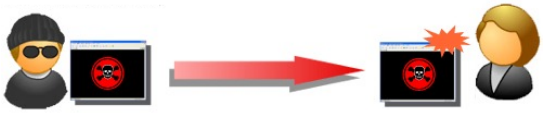
Na verdade, não se trata de um problema de segurança, mas para alguns utilizadores pode ser considerado invasão da privacidade.

Spam

O *spam* é o termo utilizado para designar o tráfego de mensagens de correio electrónico não solicitadas que enchem as caixas de correio dos utilizadores. Trata-se de uma forma de difusão em massa de correio electrónico não desejado.

Hoaxes - boatos

Os *hoaxes* (boatos) são comuns na Internet e não são mais do que mensagens de correio electrónico que possuem conteúdos alarmantes ou falsos. De entre os *hoaxes* típicos destacam-se as correntes ou pirâmides, que se referem a pessoas ou crianças que estão a morrer de cancro, etc..



Este tipo de mensagens de correio electrónico são criadas com o intuito de espalhar desinformação pela Internet. Normalmente, os criadores deste tipo de mensagem têm como objectivo verificar o quanto e quão depressa se espalha a mensagem criada.

capítulo 4

Alguns conselhos práticos

- **Introdução**
- **Palavras-passe**
- ***Banking online***
- **Correio electrónico**
- **Actualizações**
- ***Backup* - cópias de segurança**
- **Algumas regras básicas da segurança**

FUNDAÇÃO para a DIVULGAÇÃO das TECNOLOGIAS de INFORMAÇÃO

Introdução

Neste capítulo serão abordados alguns conselhos e sugestões práticas para melhorar a utilização do computador, no contexto da segurança informática.

Palavras-passe (*passwords*)

Um dos elementos que se deve ter em conta ao nível da segurança é a questão das palavras-passe (*passwords*), pois é através destas que um utilizador efectua a sua autenticação em diferentes aplicações, como por exemplo o correio electrónico.

Nunca deve fornecer uma palavra-passe a outras pessoas pois estas poderiam utilizá-la para efectuar acções em seu nome.

Existem alguns cuidados a considerar na escolha de uma palavra-passe, tais como:

- **Nunca utilizar dados pessoais na elaboração de uma palavra-passe, como nome, número do BI ou de outros documentos, matrículas, números de telefone, datas (nascimento, casamento, etc.), ou qualquer outro dado relacionado com o utilizador em questão;**
- **Não utilizar palavras que façam parte de dicionários pois existe *software* que tenta descobrir palavras-passe através de inúmeras tentativas utilizando palavras existentes em dicionários de diversos idiomas (percorrendo palavra a palavra cada dicionário);**
- **Uma palavra-passe forte deverá ter pelo menos 7 caracteres;**
- **Utilizar uma combinação de letras (maiúsculas e minúsculas), algarismos e símbolos (#$%&!). Um exemplo de uma palavra-passe forte e segura será *X#bs7pH3*;**

- **Não utilizar a mesma palavra-passe para diversos fins, ou seja, para cada aplicação (correio electrónico, *banking online*, etc.) utilizar uma palavra-passe distinta. Ao utilizar a mesma palavra-passe para diversos fins, se alguém mal intencionado descobrir essa palavra-passe, os danos poderão ser mais vastos;**
- **Trocar de palavra-passe regularmente, ou seja, não a manter inalterável por longos períodos de tempo. Normalmente, não se deve manter a mesma palavra-passe por mais do que dois a três meses.**

Banking online

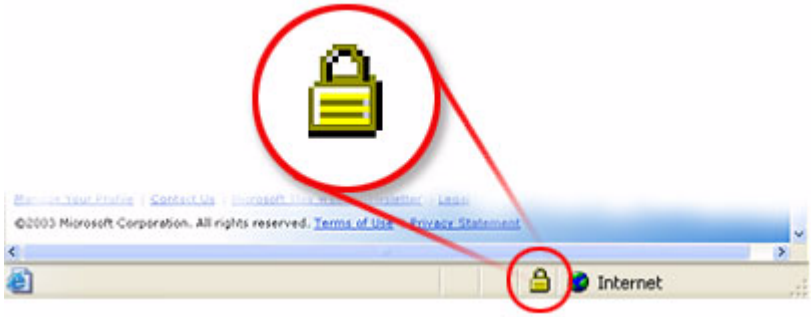
O termo *banking online* significa aceder ao seu banco através da Internet. Esta forma de acesso ao banco tem vindo a ter um enorme acréscimo de utilização nos últimos tempos e não é difícil perceber porquê. O facto de poder pagar serviços, efectuar transacções, etc., a qualquer hora e na comodidade do lar, representa vantagens e evita perdas de tempo.

Apesar das vantagens inerentes à utilização do *banking online*, é por demais evidente que é necessário conhecer o mais possível a segurança dessas transacções.

Aqui ficam alguns concelhos para aceder ao seu banco de forma segura:

- **Certificar-se da reputação do banco;**
- **Conferir a declaração de privacidade antes de efectuar qualquer transacção;**
- **Escolher uma palavra-passe forte e segura, e mantê-la secreta;**
- **Imprimir um registo da transacção efectuada pela Internet, mantendo assim um suporte físico do registo em papel;**

- **Aceder apenas ao *banking online* com tecnologias de segurança adicionais (ver figura), o endereço deverá começar por https://...**



Exemplo da identificação de um site com tecnologias de segurança adicionais

Correio electrónico

Quando se recebem mensagens de correio electrónico, existe o risco de algumas dessas mensagens serem perigosas (*worms*, vírus, *spam*, etc.), pelo que se deve ter bastante cuidado antes de abrir as mensagens. Em particular, deve ter-se muito cuidado com os anexos: deve, apenas, abrir anexos de mensagens das quais conhece os remetentes (e, se possível, o conteúdo).

Para facilitar um pouco, também se podem utilizar regras para a separação das mensagens em pastas, dependendo do seu assunto ou remetente.

Actualizações de software

É boa prática manter sempre actualizado o *software* que se encontra instalado no computador. Caso utilize o Windows XP, pode optar por activar as actualizações automáticas.

Ao manter o computador actualizado estará a reduzir o risco de vir a ter problemas de segurança.

Backup - cópias de segurança

Para garantir uma maior segurança de toda a informação importante para o utilizador, aconselha-se a realização de *backups* (cópias de segurança) de forma regular.

Este procedimento consiste em copiar a informação de trabalho do utilizador (pastas e ficheiros) para outro suporte (CDs, DVDs, *tapes*, etc.).

Ao efectuar cópias de segurança pode evitar muitos aborrecimentos, pois em caso de problemas com o computador, quer tenham sido causados por vírus quer sejam avarias imprevistas de *hardware*, existirá sempre uma cópia de segurança com a informação necessária.

Algumas regras básicas de segurança

De seguida apresenta-se uma lista com algumas das regras básicas de segurança para os utilizadores:

1. Manter todo o *software* actualizado, em particular o sistema operativo;
2. Possuir uma *firewall* instalada no computador;
3. Possuir um *software* antivírus instalado e actualizado;
4. Efectuar cópias de segurança regularmente;
5. Escolher palavras-passe fortes e seguras, bem como alterá-las regularmente;
6. Não facilitar palavras-passe ou códigos de acesso a ninguém;
7. Não escrever as palavras-passe e outros códigos de acesso em documentos e guardá-los no computador;
8. Não devem abrir-se mensagens de correio electrónico de origem desconhecida. Deve certificar-se quanto à autenticidade e credibilidade das mensagens de correio electrónico recebidas, sobretudo quando não foram solicitadas. Ter em especial linha de conta as mensagens de correio electrónico com anexos;
9. Ao aceder a *banking online*, certificar-se que se trata de um *site* seguro através do respectivo símbolo que surge na **Barra de estado** do *browser*.

apêndice A

Checklist de segurança

- **Introdução**
- ***Checklist* de segurança**

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

Introdução

Neste apêndice, o utilizador poderá efectuar uma verificação das medidas que já tomou para melhorar a segurança do computador, permitindo assim verificar qual o risco que ainda corre e quais as medidas que ainda deverá tomar.

Checklist de segurança

Assinale, na seguinte lista de verificação, as acções que efectua para proteger o seu computador:

1. Palavras-passe (*passwords*)

- ☐ Utilizo palavras-passe diferentes nas várias aplicações (correio electrónico, *banking online*, etc.);
- ☐ As minhas palavras-passe não contêm nomes, datas ou outros dados pessoais;
- ☐ As minhas palavras-passe têm mais de 7 caracteres e são formadas por letras (maiúsculas e minúsculas), algarismos e símbolos;
- ☐ Altero as minhas palavras-passe frequentemente;
- ☐ Não guardo as palavras-passe e outros códigos de acesso em documentos no computador.

2. Problemas gerais de segurança

- ☐ O sistema operativo e demais programas encontram-se actualizados;
- ☐ Tenho um *software* antivírus instalado e actualizado;

- ☐ A *firewall* está instalada e a funcionar correctamente;
- ☐ Ao aceder a *banking online*, certifico-me de que se trata de um *site* seguro através do ícone 🔒;
- ☐ Efectuo cópias de segurança de forma regular e periódica.

3. Correio electrónico

- ☐ Verifico sempre a proveniência das mensagens de correio electrónico e não abro quando são de proveniência duvidosa ou desconhecida;
- ☐ Não abro qualquer anexo, de uma mensagem de correio electrónico, sem antes verificar a sua proveniência e o seu possível conteúdo.

apêndice B

Glossário

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

ActiveX - Um conjunto de tecnologias que permite que os componentes de *software* interajam num ambiente de rede, independentemente da linguagem com o qual os componentes foram criados.

Antivírus - *Software* especificamente desenvolvido para detectar, anular e eliminar vírus.

Aplicação Java - Uma classe Java que é carregada e executada por uma aplicação Java já executada como, por exemplo, um *browser*. As aplicações Java podem ser transferidas e executadas por um *browser* com capacidade para interpretar a linguagem Java como, por exemplo, o Microsoft Internet Explorer. As aplicações Java são frequentemente utilizadas para adicionar efeitos multimédia e interactividade a páginas Web como, por exemplo, apresentações de vídeo, animações, calculadoras, relógios em tempo real e jogos interactivos. As aplicações podem ser activadas automaticamente quando a respectiva página é apresentada num *browser* ou podem necessitar de alguma acção por parte do visitante do *site* como, por exemplo, clicar num elemento da página.

Browser - *Software* que localiza e permite aceder ao conteúdo de páginas Web, por exemplo, o **Internet Explorer**.

Correio electrónico - Serviço de envio e recepção de mensagens escritas que funciona na Internet.

Download - Processo de transferência de ficheiros de um servidor na Internet para o computador local (do utilizador).

E-mail - O mesmo que correio electrónico.

Endereço - Local electrónico onde se guarda determinada informação. No caso do correio electrónico, corresponde à caixa postal do utilizador.

Endereço IP (endereço *Internet Protocol*) - Um número binário de 32 *bits* que identifica, de modo exclusivo, um equipamento ligado à Internet. Um endereço IP é composto por 4 números (cada um varia entre 0 a 255) separados por um ponto; por exemplo: 192.168.1.50.

Engenharia social - Método de ataque onde um indivíduo ou organização faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do utilizador, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

FAQ (perguntas mais frequentes) - Um documento que apresenta as questões e respectivas respostas correntes sobre um determinado assunto.

Firewall - Componente de *hardware* e/ou *software* que fornece um sistema de segurança que impede o acesso não autorizado do exterior a um computador ou a uma rede interna.

FTP (*File Transfer Protocol*) - protocolo utilizado na Internet, para a transferência de ficheiros.

Hiperligação (*hyperlink*) - Consiste num elemento de um documento electrónico (documento do Word, página Web, etc.) que se encontra ligado a outro local do mesmo documento ou a outro documento diferente.

HOAX (boato) **-** Mensagem recebida por correio electrónico, cujo conteúdo é alarmante e, em regra, falso. Pode ser visto como um vírus social, pois utiliza a boa fé dos utilizadores para se propagar, sendo esse o seu principal objectivo.

HTML (*HyperText Markup Language*) - linguagem utilizada para descrever o formato de apresentação do conteúdo de páginas Web.

HTTP (*HyperText Transfer Protocol*) - Protocolo de comunicação de dados utilizado na Web. Este protocolo define como é que é que a informação é formatada e transmitida entre *browsers* e

servidores Web. Define, igualmente, que operações os *browsers* e os servidores Web deverão realizar em resposta a determinados comandos.

Internet - conjunto de inúmeras redes de comunicação de dados que ligam milhões de computadores, a nível mundial.

ISP (*Internet Service Provider*) - empresa de serviços que fornece acesso à Internet.

Palavra-passe (*password***) -** Conjunto de caracteres, de conhecimento único do utilizador, utilizados no processo de validação de sua identidade, assegurando que ele é realmente quem diz ser.

Site (sítio em português) - Um *site* é uma localização na Internet. Por exemplo, um *site* FTP é um computador que disponibiliza o serviço de FTP (idêntico a FTP server); um Web *site* é um conjunto de páginas Web relacionadas entre si e mantidas pela mesma entidade.

Spam - Termo usado para se referir as mensagens de correio electrónico não solicitadas, que geralmente são enviados para um grande número de pessoas. Quanto ao conteúdo, este é exclusivamente comercial. Este tipo de mensagens também é referenciada como ***UCE*** (*Unsolicited Commercial Email*).

TCT/IP (*Transmission Control Protocol / Internet Protocol*) - protocolo de comunicação de dados utilizado na Internet.

Trojan (cavalo de Tróia**) -** Programa que além de executar funções para as quais foi aparentemente concebido, também executa outras funções normalmente maliciosas e sem o conhecimento do utilizador.

Vírus - Porção de código escrita com a intenção de se replicar. Um vírus espalha-se de computador em computador através de programas ou documentos, quer através disquetes, CDs ou por correio electrónico. Um vírus pode danificar a informação guardada no computador, o *software* ou mesmo o *hardware*.

Worm - Uma subclasse de vírus. Um *worm* espalha-se em acção directa do utilizador através das redes, normalmente através da lista de contactos do utilizador, enviando-se automaticamente para todas as pessoas dessa lista de contactos. Um *worm* pode implicar diversos problemas, como o consumo de memória, largura de banda, ou mesmo implicar o mau funcionamento do computador.

WWW (*World Wide Web*) - conjunto de todas as páginas Web existentes na internet.

apêndice C

Notas

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

apêndice D

Cursos disponíveis nos CDTI

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

Cursos disponíveis nos

Centros de Divulgação das Tecnologias de Informação

- Windows 98, Me, 2000 e XP - Sistema Operativo
- Word 2000, 2002-XP e 2003 - Processador de Texto
- PowerPoint 2000, 2002-XP e 2003 - Apresentações Electrónicas
- Excel 2000, 2002-XP e 2003 - Folha de Cálculo
- Access 2000, 2002XP e 2003 - Gestão de Bases de Dados
- Iniciação à Internet
- Utilização Avançada da Internet
- FrontPage 2000, 2002-XP e 2003 - Edição de Sites
- Outlook 2000, 2002-XP e 2003 - Gestão de Informação Pessoal
- Publisher 2000 - Publicações Electrónicas
- Flash 5 e MX - Animações para a Internet
- Edição de Páginas WWW - Criação de Páginas em HTML
- Edição de Sítios WAP
- Director 6.5 e 7.0 - Criação de Aplicações Multimédia
- Project 2000, 2002 e 2003 - Gestão de Projectos
- CorelDRAW 8.0 e 9.0 - Ilustração Gráfica
- AutoCAD 2D e 3D nas versões 2000, 2002, 2004 e 2005 - Desenho Assistido por Computador
- WinJúnior - Windows para os mais Jovens
- OfficeJúnior - Office para os mais Jovens
- Física, Movimento e Computadores - Estudo e Simulação de Movimentos

- Matemática e Computadores - Actividades Didácticas sobre Matemática
- ABC da Astronomia - Iniciação ao estudo da Astronomia
- Técnicas de Programação
- Programação em Visual Basic 6.0
- ASP.NET
- Curso de Formação Pedagógica Inicial de Formadores

Solicite informações sobre outros cursos no CDTI da sua localidade ou visite o sítio fdti.juventude.gov.pt.

apêndice E

Títulos editados pela FDTI

FUNDAÇÃO para a *DIVULGAÇÃO* das *TECNOLOGIAS* de *INFORMAÇÃO*

Títulos editados pela FDTI

ABC da Astronomia
ASP.NET
AutoCAD 11 - vol. 1 e 2
AutoCAD 14
AutoCAD 2000
AutoCAD 2004
AutoCAD 2005 - 2D
AutoCAD 2005 - 3D
Base de Dados dBase III Plus
Base de Dados Access 7.0, 97, 2000, 2002 - XP e 2003
BASIC
Clipper Vol.1
CorelDRAW 8
CorelDRAW 9
Desenho e Apresentações PowerPoint 97, 2000, 2002 - XP e 2003
Director 6.5
Director 7
Edição de Sítios WAP
Electrónica Digital E A C
Física, Movimentos e Computadores
Flash MX
Folha de Cálculo Excel 4.0, 97, 2000, 2002 - XP e 2003
Folha de Cálculo Lotus 123
FrontPage 98, 2000, 2002 - XP e 2003
Iniciação aos Computadores
Inteligência Conectiva
Introdução às Tecnologias de Informação e Comunicação
Matemática e Computadores
Métodos e Técnicas Pedagógicas

MS-DOS 5.0/6.0
MS-DOS Tópicos Avançados
OfficeJúnior
Outlook 97, 98, 2000, 2002 - XP e 2003
Pascal vol.1
Processador de Texto DisplayWrite 4
Processador de Texto Word 2.0, 6.0, 97, 2000, 2002 - XP e 2003
Processador de Texto Word 5.5
Processador de Texto Word 7.0
Processador de Texto WordStar
Producer
Project 98, 2000, 2002 e 2003
Publisher 2000
Robótica Sistema Rhino e ROB 3i
Segurança
Técnicas de Programação
Visual Basic 6
Windows 3.1, 95, 98, Me, 2000 Professional e XP
WinJúnior
WWW Edição de Páginas

Consulte a lista completa de títulos editados, e em preparação, em fdti.juventude.gov.pt.