Instituto Politécnico de Santarém

Escola Superior de Educação

Curso de Educação Social

1º Ano Ensino Diurno

Tecnologias de Informação e Comunicação-TIC

Docente: Ana Loureiro

Segurança Informática

Discentes:

- Ana Rita Gaspar, nº120230040
- Ana Sofia Vau, nº120230043
- Cátia Marmelo, nº 120230030
- Daniela Pedro, nº120230031

Índice

Introdução

Na disciplina de TIC I (Tecnologias da Informação e Comunicação), foi proposto ao nosso grupo uma série de temas alusivos à disciplina. No entanto, o nosso grupo optou por escolher o tema relativo à "Segurança Informática", uma vez que foi aquele que nos suscitou mais interesse.

O trabalho aborda a temática das redes informáticas, como a Internet, falando sobre a sua segurança e sobre os seus perigos, como os vírus e a pirataria existente. Dada a escassez deste tipo de informação em meios bibliográficos sobre este tema, baseamo-nos em sítios da internet.

Quanto à estrutura do trabalho, ele aborda subtemas como a segurança informática, navegação segura, vírus e pirataria.

Numa primeira parte do trabalho debruçamo-nos sobre a segurança informática, a sua definição e conceito. Falamos ainda, sobre alguns objetivos da segurança e as causas que levam à exposição de dados de forma insegura. A segunda parte aborda a questão de navegação segurança na internet. Falamos de cuidados e medidas a tomar de forma a proceder a uma navegação sem preocupações por parte do utilizador.

Por fim, expomos alguma informação sobre os vírus que afetam os computadores, a forma como se capturam, e medidas que se podem tomar para os evitar. Abordamos também a pirataria e a sua ilegalidade.

1. Conceito:

Segurança Informática está ligada à proteção de um conjunto de dados, com o objetivo de preservar o valor que possuem para um indivíduo ou para uma organização. O conceito aplica-se em todos os aspetos de proteção de informações e dados. O conceito de Segurança Informática está relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

O sistema de informação define-se geralmente como o conjunto dos dados e dos recursos materiais e *software* da empresa que permite armazená-los ou fazê-los circular. O sistema de informação representa um património essencial da empresa, que convém proteger.

A segurança informática visa geralmente cinco objectivos principais:

- A **integridade**, ou seja, garantir que os dados são efetivamente os que crê ser;
- A **confidencialidade**, consistindo em assegurar que só as pessoas autorizadas têm acesso aos recursos trocados;
- A **disponibilidade**, permitindo manter o bom funcionamento do sistema de informação;
- **Não repudiação**, permitindo garantir que uma transação não pode ser negada;
- A **autenticação**, consistindo em assegurar que só as pessoas autorizadas têm acesso aos recursos.

Exemplo: Com o desenvolvimento da utilização de Internet, cada vez mais empresas abrem o seu sistema de informação aos seus parceiros ou aos seus fornecedores, é por isso necessário conhecer os recursos da empresa a proteger e dominar o controlo de acesso e os direitos dos utilizadores do sistema de informação. O mesmo no que diz respeito à abertura do acesso à empresa na Internet. Além disso ao permitir os indivíduos ligarem-se ao sistema de informação a partir de qualquer lugar, os indivíduos são levados a "transmitir" uma parte do sistema de informação para fora da infraestrutura protegida da empresa.

2. Noções sobre segurança Informática

Se ligar à Internet, permitir que outras pessoas utilizem o seu computador ou partilhar ficheiros com outros utilizadores, deve tomar medidas para proteger o computador. Porque existem criminosos informáticos (hackers) que atacam computadores. Estas pessoas podem atacar diretamente, entrando no computador através da Internet e roubar as suas informações pessoais, ou indiretamente, criar um *software* malicioso concebido para danificar o computador.

Para prevenir estas situações deve:

Verificar o estado de segurança com o Centro de Segurança do Windows:

O Centro de Segurança do Windows é o ponto central da segurança do computador. Esta funcionalidade mostra o estado de segurança atual do computador e apresenta conselhos sobre as ações que deve efetuar para tornar o computador mais seguro.

O Centro de Segurança verifica estes aspectos de segurança essenciais no computador:

- ***Firewall*.** Uma *firewall* pode ajudar a proteger o computador, impedindo que os hackers ou software malicioso consigam aceder-lhe.
- **Actualização automática.** O Windows pode procurar regularmente atualizações para o computador e instalá-las automaticamente.
- **Proteção contra *malware* (*software* malicioso).** O *software* antivírus pode ajudar a proteger o computador contra vírus, *worms* e outras ameaças de segurança. O *software anti-spyware* pode ajudar a proteger o computador contra *spyware* e outro software potencialmente indesejado.
- **Outras definições de segurança.** O Centro de Segurança verificar as definições de segurança da Internet e se o Controlo de Conta de Utilizador está ou não ativado.

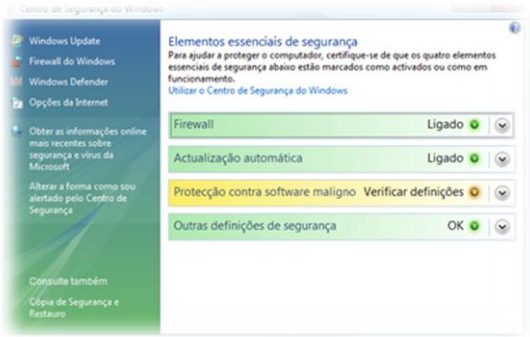

Fig.1-Centro de Segurança do Windows

3. Alertas de segurança:

Se o Windows detetar que o computador pode necessitar de segurança avançada em qualquer uma das áreas de segurança, será apresentada uma notificação sempre que iniciar sessão até que o problema seja corrigido. As notificações são apresentadas na área de notificação da barra de tarefas.

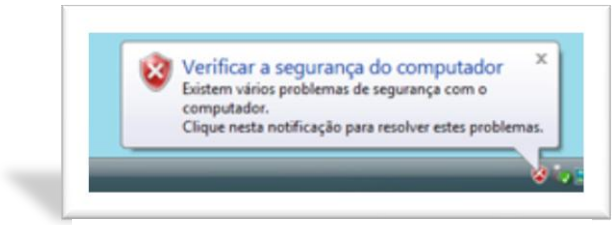

Fig.2-Notificação de Segurança

4. Firewall:

Uma *firewall* é *software* ou *hardware* que verifica as informações recebidas a partir da Internet ou de uma rede e que recusa ou permite a respectiva passagem para o computador, dependendo das definições da *firewall*. Deste modo, uma *firewall* ajuda a impedir que *hackers* e software malicioso acedam ao computador. A *Firewall* do *Windows* está incorporada no *Windows* e é ativada automaticamente.

Se executar um programa, tal como um programa de mensagens instantâneas ou um jogo em rede que necessite de receber informações a partir da Internet ou de uma rede, a *firewall* pergunta-lhe se pretende bloquear ou desbloquear (autorizar) a ligação. Se optar por desbloquear a ligação, a *Firewall* do *Windows* cria uma exceção para que a *firewall* não o incomode quando esse programa necessitar de receber informações posteriormente.

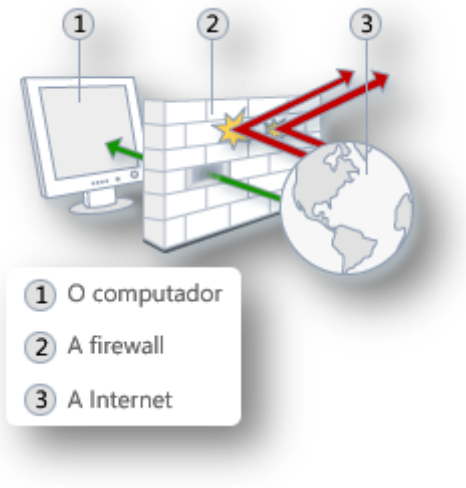

Fig.3-Como funciona uma *firewall*

5. Vírus

- ✓ Deriva do latim "*virus*", que significa veneno.

❖ Vírus Informático

Contaminação ou série de contaminações parasitas introduzidas num *software* (programa) que poderão provocar inúmeros problemas no funcionamento do computador. Ou seja, um vírus informático é um programa de *software* que se difunde de computador para computador, afetando assim o funcionamento do mesmo. Existem diversos tipos de vírus que podem influenciar nas mais diversas tarefas do computador, ou até mesmo no seu todo. Pode eliminar dados guardados num computador, pode usar o nosso correio eletrónico como via de propagação destes mesmos vírus ou na pior das hipóteses, eliminar todas as informações, dados, trabalhos, entre outros que estejam guardados no disco rígido do computador.

❖ Formas de propagação de Vírus Informático

Existem diversas formas dos vírus informáticos se propagarem, entre elas:

- ✓ Correio eletrónico (anexos em mensagens [imagens, cartões de felicitação, ficheiros de som, vídeo, entre outros] ou mensagens instantâneas);
- ✓ Transferências de ficheiros executadas através da Internet;
- ✓ Colocar dispositivos de entrada (*pendrives,* entre outros) em computadores já contaminados;
- ✓ Utilização de *softwares* pirateados.

❖ Sintomas de existência de Vírus no computador

De forma a combater eficazmente quaisquer sintomas (que mais tarde poderão vir a ser confirmados) da existência de vírus, devemos ter sempre em atenção a aquisição de um *software* antivírus atualizado. Contudo, devemos ter em conta os seguintes sintomas:

- ❖ Computador mais lento que o normal;
- ❖ Bloqueios frequentes;
- ❖ Falhas de sistema e consequentemente reinício do computador;
- ❖ Falha a nível de funcionamento de aplicações instaladas;

- Inacessibilidade a unidades ou dispositivos no computador;
- Falha na impressão de documentos;
- Receção de mensagens de erro;
- Menus ou caixas de diálogo distorcidos;
- Impossibilidade de utilização/instalação do programa de antivírus sem razão aparente;
- Aparecimento de novos ícones no ambiente de trabalho;
- Reprodução de sons estranhos através dos altifalantes do computador;
- Desaparecimento de programas que não foram eliminados pelo utilizador;
- Entre outros.

Proteção contra vírus:

Os vírus, worms e Trojans são programas criados por hackers que utilizam a Internet para infectar computadores vulneráveis. Os vírus e worms podem replicar-se entre computadores, enquanto que os Trojans entram num computador ocultando-se no interior de um programa aparentemente legítimo, tal como uma proteção de ecrã. Os vírus, worms e Trojans destrutivos podem apagar informações do disco rígido ou desativar totalmente o computador. Outros não causam danos diretos, mas prejudicam o desempenho e estabilidade do computador. Os programas antivírus analisam as mensagens de correio electrónico e outros ficheiros existentes no computador para detectar a existência de vírus, worms e Trojans. Se for encontra um, o programa antivírus coloca-o em quarentena (isola-o) ou elimina-o totalmente antes que este danifique o computador e os ficheiros. O Windows não tem um programa antivírus incorporado, mas o fabricante do computador poderá ter instalado um.

6. Worm

- ✓ ***Significa "verme", é um programa semelhante a um vírus.***

Basicamente, a diferença entre o Vírus e o Worm é que o primeiro referido infeta um programa e precisa desse mesmo programa para se propagar e o segundo referido é completo, consequentemente não necessita de outro programa para se propagar.

- Um *Worm* pode ter vários objetivos:

- ✓ Auto-replica de programas;
- ✓ Apagar pastas;

- ✓ Enviar e-mails maliciosos automáticos;
- ✓ Entre outros.

O *Worm* é perigoso porque pode tornar o computador vulnerável, pois poderá provocar danos generalizados, quer a nível de computador, quer a nível de Internet no seu geral (o *Mydoom* é um exemplo de *Worm* que afetou a utilização da Internet no seu geral).

Curiosidades:

- ❖ O primeiro *Worm* que teve mais impacto foi o *Morris Worm*, executado por *Robert T. Morris Jr*. no Laboratório de Inteligência artificial do *MIT (Instituto de Tecnologia de Massachusetts)*. Teve início em 2 de novembro de 1988 e rapidamente infetou um grande número de computadores pela Internet.
- ❖ Existem *Worms* uteis, por exemplo os *Worm Nachi* procuravam e instalavam "remendos" *(patches)* diretamente do *site* da Microsoft de forma a corrigir erros causados por outros *Worms.*

7. Trojan

- ✓ Deriva do termo "Cavalo de Troia" e atua tal como a lenda do cavalo de Troia, entra no computador e abre uma porta para uma possível invasão. É relativamente fácil de ser enviado: clica-se no ID do computador e envia-se para qualquer outro computador.

O *Trojan* é geralmente usado para destruir o computador. Inicialmente consistia em algo simples, como por exemplo, entrar num *site* à partida fidedigno, digitar senhas e e-mails e esse mesmo site "rouba" as informações colocadas. Mas o conceito de *Trojan* já evoluiu. Este tipo de Vírus ou *Malware* aparece muitas vezes em programas que nos parecem ser legítimos e fidedignos.

Este tipo de vírus divide-se então em duas partes:

- ✓ *O servidor* que se instala e esconde no computador do utilizador, dentro de uma pasta;
- ✓ *O cliente* que tem acesso ao computador a partir do momento em que o servidor abre a pasta com o *Trojan.* Por sua vez, o cliente irá enviar ordens ao servidor de forma a executar quaisquer operações malignas no computador do utilizador.

Divide-se também em dois tipos:

- ✓ *Keylogger* é um *spyware* cuja finalidade é registar tudo o que é escrito de forma a obter *passwords.*
- ✓ *Backdoor* que é uma falha de segurança que pode existir num programa de computador ou num sistema operativo, que permite a invasão do sistema por um *cracker* de forma a que obtenha o controlo total do computador.

Curiosidades:

- ❖ O *Trojan* instala-se no computador com um simples *e-mail* do tipo *spam* apelando ao utilizador que abra o e-mail de forma a que possa ter acesso a conteúdos (com um link onde o vírus fica hospedado) como: fotografias de famosos, músicas, entre outros.

8. Sintomas de *Worms* e *Trojans* através do e-mail

- ✓ Criação de várias cópias do mesmo ficheiro (poderá esgotar o espaço de memória do computador);
- ✓ Envio de uma cópia de ficheiro infetado a todos os contactos da lista de *e-mail*;
- ✓ Reformatação do disco rígido (eliminação de programas e ficheiros do computador, consequentemente);
- ✓ Instalação de programas ocultos (*software* pirata);
- ✓ Redução de segurança (acesso ao e-mail por estranhos);

9. Forma de proteger o computador contra possíveis vírus:

- ✓ Manter sempre o sistema operativo atualizado, assim como o anti-vírus e o *anti-spyware*.

10. Defesa em profundidade

Este princípio pretende dificultar o acesso aos recursos importantes e recorre a vários mecanismos de defesa como:

- ✓ Registo Detalhado das atividades.
- ✓ Mecanismos de Alerta para situações “estranhas”.
- ✓ Os mecanismos de defesa estruturam-se em camadas pelo que possuem independência uns dos outros.

Um sistema vulnerável pode ser razoavelmente fortificado e protegido através de uma adequada defesa em profundidade mas não vai eliminar completamente o risco de aproveitamento das fraquezas do sistema.

II. Noção de Vulnerabilidade

Uma vulnerabilidade decorre de deficiência (s) do *software* devido a programas complexos com inúmeras interações entre si e o sistema operativo ou a um software mal feito, devido ao cumprimento de prazos que obrigam a que o software tenha de estar pronto a numa determinada data e não tenha sido sequer totalmente testado e revisto. Pode ainda acontecer que os fabricantes de software que recorram a programadores com formação inadequada e por conseguinte os cliente estarão mais susceptíveis aos riscos.

As vulnerabilidades afetam:

- ✓ Sistemas operativos com efeitos globais e muitos gravem para o sistema;
- ✓ Aplicação de sistemas que geram efeitos localizados e graves para o sistema e aplicações de utilizadores que geram efeitos localizados e graves para o utilizador;
- ✓ Vulnerabilidades e perturbação de funcionamento.

Uma vulnerabilidade passível de perturbação de funcionamento pode permanecer oculta durante muito tempo, esta perturbação de funcionamento pode ter origem no local (por um utilizador do sistema computacional), através da rede local (por um utilizador de uma plataforma da rede local) ou rede externa (por um utilizador de uma plataforma de uma rede externa)

As consequências de uma perturbação de funcionamento variam em termos de duração temporal (de curta até prolongada) de efeito sobre o sistema (de nulo até à catástrofe) e em termos de exploração do sistema (de nula até à subversão do sistema).

12. Navegação Segura

Para obtermos uma navegação segura na internet, no caso de informações pessoais, contas ou vírus devemos tomar as seguintes precauções:

- ✓ Sair de um sítio com autenticação usando sempre o *logout*, o *logoff* ou o sair. Caso contrário, qualquer pessoa pode entrar em contas que não lhe pertence, e criar também senhas com o máximo de complexidade possível, de forma a ser difícil de serem descobertas, a melhor forma é misturar letras maiúsculas e minúsculas e números. É imprescindível mudar de senha periodicamente, pois apesar de se criar senhas difíceis de serem descobertas, deve-se troca-las com frequência;

- ✓ Usar navegadores diferentes. O uso frequente do Windows e da navegação no Internet Explorer provoca uma infinidade de pragas digitais que prejudicam o sistema informático do computador;

- ✓ Ter cuidado com as descargas da internet (*download*) pois é essencial ter em atenção à finalização da descarga e ver se o arquivo não tem nada de estranho, em termos de descrições suspeitas, informações com tamanho reduzido, pois é muitas vezes desta forma disfarçada que os vírus se infiltram no computador;

Fig.4- Password

- ✓ Ter muita atenção quando se usa MSN, GTalk, YAHOO, MESSENGER, entre outras aplicações de conversação instantânea. É muito comum encontrar vírus que exploram este tipo de serviços. Estes vírus são capazes de durante uma conversa com um contacto, enviar mensagens automáticas que contem ligações para vírus, ou outros programas maliciosos. Ao receber uma ligação para um sítio que não se está à espera é necessário confirmar quem o enviou e caso não conheça não se deve clicar, mas sim informar o contacto que o seu computador pode estar com um vírus. É muito comum acontecer isto também quando recebemos correio electrónico;

- ✓ Ao fazer compras na internet ou usar sítios de bancos é preciso ter sempre em atenção se o sítio é conhecido. Ao utilizar cartões de crédito ou digitar números de identificação bancária (NIB), é fundamental fazê-lo em segurança e evitar fazer esse tipo de movimentos em computadores públicos;

Fig.5- Aviso

✓ Atualizar todos os programas pois as novas versões dos programas contêm novas correções para falhas de segurança. Este procedimento é essencial no caso do antivírus.

13. Formas de Evitar o Hacking

○ HTTPS (HyperText Transfer Protocol Secure)

Este protocolo é usado frequentemente nos días de hoje para garantir segurança na comunicação na internet. Basicamente trata-se de uma nova camada de segurança em cima do HTTP normal. HTTPS permite autenticação do cliente e do servidor para onde estamos a comunicar de modo a que tenhamos a certeza que estamos a comunicar para o sítio certo e nos estejam a responder para o sítio certo também, evitando assim que pessoas de fora consigam ter acesso a informações restritas. Esta segurança de comunicação é feita através da encriptação bidirecional entre o cliente e o servidor. Antigamente este protocolo era apenas utilizado em transferências bancárias ou atividades dessa natureza porém, nos dias de hoje, já e utilizado nos mais variados sítios existindo até mesmo no popular Facebook a opção de navegar através deste protocolo.

○ Criptografia

Na criptografia, a encriptação é o processo de codificar mensagens (ou informação) de modo a que os hackers não a consigam ler, mas as pessoas autorizadas (para quem mandamos) possam. Esta encriptação é feita partir de dois pares de chaves, uma pública e outra privada. À chave pública toda a gente tem acesso, mas esta apenas serve para encriptar. No entanto, a desencriptação da mensagem só pode ser feita a partir da chave privada do elemento que vai receber a mensagem pelo que apenas ele a consegue ler.

14.Pirataria na internet

Pirataria na internet é o download ou a distribuição não autorizada de conteúdos protegidos por direitos autorais, tais como filmes, músicas, programas de televisão, vídeo-clipes ou programas de computador, com ou sem intuito de lucro. A distribuição e o download ilegal desses conteúdos se dá de diversas formas, inclusive por meio de redes P2P (peer-to-peer) de compartilhamento de arquivos, como e-donkey, bit torrent e gnutella, e por meio de discos virtuais (como rapidshare e megaupload). Nessas redes e sistemas, um único arquivo disponibilizado pode resultar em milhões de downloads ilegais.

A Internet também é amplamente utilizada para a venda de obras musicais e audiovisuais reproduzidas ilicitamente, contexto em que ganham relevância redes sociais e sites de leilão, constantemente sob monitoramento.

Entre as várias formas de pirataria temos:

- **Pirataria de utilizador final -** Ocorre quando os internautas fazem cópias adicionais de programas sem autorização. Estão incluídas as cópias fortuitas realizadas por colaboradores de determinadas empresas que não monitorizam o número de licenças instaladas e adquiridas pela empresa.
- **Venda não autorizada -** Ocorre quando o pirata informático faz a respetiva descarga dos programas, filmes, séries, músicas, etc. E o coloca para venda ao público.

15. Pirataria pela internet

Há numerosas operações não autorizadas a ocorrer pela internet:

- Sites piratas que disponibilizam o download gratuito dos programas, ou requisitam a troca pelo *upload* de outros programas;
- Sites de leilões via Internet que oferecem cópias falsas, desviadas, ou com quebra de direitos autorais dos programas;
- Redes peer-to-peer que permitem a transferência não autorizada de programas protegidos por direitos autorais.
- A pirataria pela Internet talvez seja o único problema a representar grande risco ao e-commerce.

16. Falsificação de Programas

É a duplicação ilegal e venda de material protegido por direitos de autor com a intenção direta de imitar o produto protegido. No caso de pacote de produtos de programas é comum encontrar cópias falsas de CDs que imitam o programa e também a sua embalagem, manuais, acordos de licença, etiquetas, cartões de registo e funções de segurança.

Conclusão

Após a elaboração do trabalho sobre "**Segurança informática, navegação segura, vírus e pirataria",** consideramos que a internet para ser segura é preciso ter alguns cuidados. É necessário, portanto, ter em conta e precaução no acesso a páginas na internet que possam induzir-nos a preencher dados pessoais, números de cartões de crédito ou outras referências que nos possam de algum modo prejudicar. Para isso é necessário garantir a integridade, a confidencialidade, a disponibilidade, a não repudiação e a autenticação.

É importante que haja consciência da vulnerabilidade que existe ao navegar-se na internet, fazendo sempre uma navegação segura, de modo a evitar males que possam causar diversos tipos de danos (monetário, por exemplo).

Para além disso, é necessário ao trocar ficheiros numa rede, devido ao mais variado número de vírus que existem. Estes podem causar alguns aborrecimentos ou a destruição completa de equipamentos integrantes no computador.

Webgrafia

- http://pt.wikipedia.org/wiki/HTTPS
- http://pt.wikipedia.org/wiki/Criptografia_de_chave_p%C3%BAblica
- http://rolan2.home.sapo.pt/trabalhos/SI.pdf
- http://support.microsoft.com/kb/129972/pt
- http://pt.wikipedia.org/wiki/V%C3%ADrus_de_computador
- http://pt.wikipedia.org/wiki/Worm
- http://pt.wikipedia.org/wiki/Keylogger
- http://windows.microsoft.com/pt-PT/windows-vista/Understanding-security-and-safe-computing
- http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o