

internet seguraopt

Acções de sensibilização/ formação – Guia
de Apoio

Última actualização a 12/01/2010

1. Possibilidades da Internet

[Slide 3]

A utilização das Tecnologias de Informação e Comunicação (TIC) tem transformado profundamente a forma como as pessoas vivem – como aprendem, trabalham, ocupam os tempos livres e interagem, tanto nas relações pessoais como com as organizações.

[Slide 4]

As Tecnologias de Informação e Comunicação são cada vez mais utilizadas para realizar tarefas de uma forma célere e cómoda. Hoje, através da Internet, já é possível:

- Efectuar transacções financeiras, como por exemplo bancárias (consulta de saldos ou transferências), compras de bens ou serviços (livros, bilhetes de espectáculo);
- Comunicar, por exemplo através de correio electrónico, mensagens instantâneas (chats e Messenger) e videoconferência;
- Armazenar e publicar informação, quer pessoal, quer institucional, como por exemplo em blogues ou sites de empresas;
- Pesquisar e aceder a informação on-line, como por exemplo jornais e revistas, horários de comboio ou viagens.

[Slide 5]

Milhões de utilizadores de todas as idades usam diariamente a Internet. A Internet, apesar de ser um meio versátil e uma fonte de inesgotáveis recursos, apresenta alguns perigos associados. O cidadão deve conhecer esses perigos, a fim de se proteger da melhor forma e educar os mais jovens a fazer o mesmo.

Ao tomar certas precauções, a sua navegação será muito mais segura e, como tal, poderá desfrutar com maior segurança as inúmeras vantagens que a Internet lhe permite.

2. Segurança no Computador

[Slide 6]

Antes de se falar na segurança da navegação e no acesso a conteúdos e ferramentas on-line, é necessário termos previamente contempladas algumas normas gerais que garantam a segurança do meio com que acedemos à Internet:

- a) Utilize uma firewall: desta forma estará a impedir o acesso ao seu computador por parte de estranhos, através da Internet; ex: ligar-se à Internet sem uma firewall é como deixar a porta de sua casa aberta;
- b) Actualize o computador: garantir que o sistema operativo e programas instalados apresentam as últimas actualizações é um importante reforço de segurança do computador; ex: tal como um carro, o computador também necessita de manutenção;
- c) Instale Antivirus e AntiSpyware: é importante que o computador tenha estes programas instalados e actualizados, já que permitem detectar, anular e eliminar os vírus e spywares informáticos; ex: o computador com um vírus instalado tem um funcionamento mais lento do que é habitual;
- d) Utilize canais seguros nas suas transacções na Internet. Se na barra de endereço do seu navegador aparecer https://, significa que está num canal seguro. Adicionalmente, deverá aparecer um ícone representando um cadeado ou uma chave;
- e) Configure o seu navegador da Internet para bloquear pop-ups. Muitas vezes pode acontecer, em sites da Internet pouco fidedignos, que os pop-ups transportem código malicioso de informações enganadoras e/ou de endereços manipulados;

- f) Certifique-se que os sites que visita são fidedignos evitando assim cair em esquemas de phishing. Nunca siga os endereços que lhe são enviados por correio electrónico, mensagens instantâneas ou em pop-ups.

3. Perigos e prevenção

[Slide 7]

Muitos dos perigos são comuns a diversas actividades que desenvolvemos na Internet. Contudo para uma melhor consciencialização de como navegar em segurança abordaremos esses perigos e prevenções analisando as actividades e os meios mais comuns. Para isso daremos uma breve descrição dos mesmos, quais os perigos que apresentam e como nos podemos prevenir/ agir perante o perigo.

a. Blogues

Embora seja considerada uma das valências das Redes Sociais Virtuais, remetemos este tema para uma secção distinta, dado apresentar características específicas e diferentes das outras Redes Sociais Virtuais.

A palavra “blogue” advém do inglês, “blog”, e é a contracção das palavras “web” e “log” (“registo na rede”, em tradução livre).

Um blogue é um sítio de Internet criado por um ou vários indivíduos (os “bloguistas”) e cujo propósito é o de partilhar informação da mais variada ordem. É tido como uma espécie de diário online, onde os utilizadores autorizados criam os seus textos (designados de “posts”), assumindo assim as suas posições relativamente a várias temáticas específicas.

A informação colocada num blogue é apresentada de forma cronológica, sendo que os artigos mais recentes são vistos em primeiro lugar e os mais antigos são disponibilizados depois.

A maioria dos bloguistas autoriza que os seus textos sejam comentados. Esta funcionalidade permite que quem acede aos blogues deixe a sua opinião ou coloque perguntas, produzindo uma interacção entre autores e leitores.

Um blogue típico pode combinar as funcionalidades do texto, imagem, vídeo e links para outros blogues ou páginas Web. Além dos blogues de conteúdos de texto, existem também blogues mais vocacionados para um determinado meio, como a fotografia (“Photolog”) ou o vídeo (“vlog”).

Os blogues têm ganho cada vez mais adeptos, assumindo até, em alguns casos, uma posição de influência política relevante. Outros blogues podem-se destinar à venda de determinados produtos, de acção solidária e até de apologia a determinadas doenças psicológicas.

Um blogue tem um modo de funcionamento bastante intuitivo, sendo esta uma das razões da sua popularidade. Para ter um blogue, o utilizador apenas tem que se registar num sítio Web que forneça este serviço e escolher algumas funcionalidades básicas, como a imagem de fundo, o nome do seu blogue e as definições de privacidade, e está pronto a começar.

O passo seguinte consiste na inserção de conteúdos no blogue, que será aquilo que o utilizador quiser que conste no mesmo. O utilizador coloca o texto, imagem, som ou vídeo que quer mostrar na caixa de texto apropriada, clica no ícone de publicação e o seu blogue está actualizado. A ordem de visualização dos assuntos num blogue é cronológica, ficando as novidades em primeiro lugar e os assuntos mais antigos no fim.

Um blogue pode ser privado ou público – quando é definido como privado, apenas as pessoas seleccionadas pelo dono do blogue têm autorização para visualizar os seus conteúdos; um blogue público é visível a todos aqueles que o desejem consultar. Além destas definições, também é possível autorizar, ou não, que outros comentem os nossos artigos, e que tipo de utilizadores o pode fazer (se apenas utilizadores registados, se autoriza comentários anónimos, etc.)

Existem bastantes entidades virtuais de criação e alojamento de blogues, muitas delas gratuitas. Regra geral, os blogues gratuitos terão menos funcionalidades que os pagos, cabendo ao utilizador a adesão a um ou outro conforme as suas necessidades.

Um facto curioso relativamente aos blogues é poderem ser um veículo de aprovação ou rejeição de um candidato a um emprego: começa a ser frequente uma entidade empregadora pesquisar o nome do candidato e ver que tipo de informações online encontra, ou seja, a forma como este se mostra no mundo virtual é tida como um reflexo do que o sujeito é no dia-a-dia. Um blogue, dado ser considerado uma forma de divulgação de opiniões pessoais, pode ser a porta de entrada (ou saída) para uma dada empresa.

[Slide 8]

Apesar de poderem ser um veículo interessante de partilha de informação e ideias, os blogues também não estão isentos de perigos, tal como outras funcionalidades da Internet.

Um utilizador informado está mais seguro, pelo que apresentamos aqui alguns dos perigos mais comuns que podem advir da utilização dos blogues:

- **SPAM, phishing ou outros**

Dado que um blogue é uma funcionalidade online, dependendo das suas definições de privacidade, pode ser alvo de SPAM, phishing ou outras formas de intrujar os menos atentos. Um blogue público e sem qualquer restrição de comentários por parte de terceiros é um alvo fácil para indivíduos ou grupos mal-intencionados.

- **Perseguições online e offline**

Dado que é uma forma de exposição pessoal, um blogue pode ser alvo de cyberbullying. Um bloguista pode verificar que algo que escreveu num artigo foi mal interpretado ou, pura e simplesmente, e sem qualquer tipo de justificação aparente, o seu blogue foi inundado de insultos, ameaças e impropérios.

Tal como noutros meios de comunicação pela Internet, o bloguista deverá evitar usar informação desnecessária de natureza pessoal.

- **Imagens**

Tal como já foi referido em algumas secções de outros perigos, a colocação de imagens pessoais na Internet pode levar outros a apropriarem-se indevidamente delas. Pense bem antes de colocar as suas imagens no blogue.

- **Blogues de apologia a doenças, discriminação, ódio, entre outros**

Como foi referido, os temas dos blogues podem ser de natureza variada. Existem blogues de apologia de comportamentos que podem levar a doenças, como a anorexia, onde se exprimem opiniões que podem levar os mais influenciáveis (por vezes, crianças e adolescentes) a iniciar e/ou manter comportamentos lesivos para a sua saúde.

Nestas situações, tal como para os outros conteúdos que envolvam riscos para os utilizadores menos preparados, como por exemplo crianças, é necessário um acompanhamento familiar adequado..

- **Responsabilização pelos conteúdos**

O bloguista é responsável pelos conteúdos inseridos no seu blogue. Contudo, esta responsabilização nem sempre é levada a sério, e muitos bloggers já foram os autores de situações lesivas para terceiros. Embora nem sempre seja propositado, é importante educar os utilizadores deste tipo de serviço para pensarem um pouco antes de colocarem algo no seu blogue, e quais as consequências desse acto, que podem até ser legais.

[Slide 9]

Alguns conselhos para uma utilização mais segura dos blogues:

- **Tipo de blogue**

Ao iniciar-se no mundo dos blogues, tenha em atenção alguns pormenores importantes: o fornecedor do serviço parece-lhe idóneo? A declaração de privacidade permite-lhe salvaguardar os seus direitos? É fornecido algum e-mail para solicitar ajuda caso necessite?

Verifique também se há custos associados ao blogue: embora haja servidores que ofereçam blogues gratuitamente, outros são pagos. Evite surpresas lendo atentamente as condições de adesão.

Por fim, defina que temas se irão enquadrar no seu blogue, a fim de ajudar os potenciais leitores a decidir se querem voltar a ler os seus artigos ou não.

- **Navegue**

Conhecer os outros blogues do servidor que pretende usar é a melhor forma de saber que funcionalidades permitem, que autores recorrem aos seus serviços e que tipos de respostas existem por parte dos leitores. Se não gostar dos blogues que vir, considere a hipótese de aderir a outro servidor.

- **Não disponibilize informação privada inadvertidamente**

Os riscos são naturalmente maiores para os mais jovens. Há predadores online que procuram nos conteúdos dos blogues as fraquezas das suas potenciais vítimas, bem como dados que os levem a elas pessoalmente.

Lembre-se que basta uma referência ao tempo (“está frio aqui em Coimbra,” por exemplo) para aproximar um pouco mais alguém indesejado.

- **Não forneça a sua palavra-passe a terceiros**

Tal como para outras funcionalidades da Internet, deverá tratar a sua palavra-passe com todo o cuidado, para evitar que o seu blogue seja apropriado indevidamente por terceiros.

- **Tenha atenção aos links que coloca**

Os links que colocar no seu blogue podem fornecer informações pessoais a seu respeito que não pretende distribuir. Por exemplo, se referir que é estudante e colocar um link da sua escola, será fácil a um eventual desconhecido intencionado encontrá-lo(a).

- **Coloque um endereço de correio electrónico genérico**

Evite moradas de e-mail que possam levar à sua identificação pessoal, como o seu nome, ou indicação do seu local de trabalho. Opte por um endereço de correio electrónico generalista que não forneça dados identificativos.

- **Defina regras e fronteiras**

Estas regras não precisam de ser explícitas, isto é, não precisam de estar à vista de todos. Defina o que, para si, é aceitável enquanto bloguista: ao permitir comentários por parte dos seus leitores, que tipos de comentários são mantidos e que comentários são apagados e desencorajados? Que tipo de linguagem vai usar nos seus artigos?

Defina também que tipo de informação vai partilhar. Um bloguista é o autor e proprietário dos conteúdos do blogue e, como tal, apenas deve escrever aquilo com que se sente confortável. Um dado importante a reter é que, caso defina o seu blogue como público, este poderá ser visto por um variado público, e a informação poderá chegar a quem não deseja, portanto, tenha em atenção ao que escreve.

Os menores devem definir os seus blogues como privados, de modo a serem apenas acedidos por pessoas autorizadas. O educador deve aceder ao blogue com alguma frequência e certificar-se que não há conteúdos inapropriados, ofensivos ou perigosos para o jovem.

- **Imagens pessoais**

Colocar imagens pessoais num blogue pode ser perigoso, pois podem permitir identificar o bloguista e os locais habituais que frequenta. Esta regra aplica-se tanto à imagem no perfil que representa o bloguista (“avatar”) como às que são colocadas nos artigos.

As crianças e adolescentes bloguistas não devem colocar quaisquer tipo de imagens pessoais na Internet, para evitar a perseguição por parte de predadores online.

Se, ainda assim, o utilizador desejar colocar imagens pessoais no seu blogue e estas focarem terceiros, deverá pedir a autorização a essas pessoas antes de o fazer.

- **Tenha planos para o caso de as coisas correrem mal**

Se, apesar de todos os cuidados, houver alguém a enviar ameaças para o seu blogue, tenha à mão um plano de acção: o que pode fazer? Quem pode contactar? Registe todos os conteúdos relevantes, tais como os artigos mencionados, o autor das ameaças e as horas das ameaças, e aja de forma a proteger-se.

Quaisquer que sejam os seus planos, envolva sempre terceiros neste processo: se achar que a sua vida está a ser prejudicada ou se sente desconfortável com o que se está a passar com o seu blogue, fale com amigos, com as autoridades apropriadas ou com outros bloguistas, que podem partilhar consigo sugestões ou experiências passadas.

- **Moderadores para os menores de idade**

Se o autor do blogue for um menor, cabe ao educador o papel de moderador. Esteja atento ao que o seu educando escreve no blogue, como o faz e que tipos de conteúdos coloca. Envolve-se nas actividades online dele e ajude-o a tomar decisões conscientes e educadas, de modo a não se colocar em risco ou provocar desentendimentos com terceiros.

b. Telemóveis

[Slide 10]

Com o advento das telecomunicações sem fios, os telemóveis tornaram-se num equipamento essencial no dia-a-dia. A chegada da Terceira Geração de telemóveis aumentou o número de serviços possibilitando, por exemplo, o registo de imagens e vídeos ou o upload de músicas, jogos ou outros conteúdos através da ligação à Internet.

Contudo, à semelhança de qualquer nova tecnologia também temos que nos confrontar com inconvenientes e perigos. Assim, temos que conhecer bem as funcionalidades dos telemóveis de Terceira Geração, para assim nos podermos proteger de utilizações abusivas e desfrutar de todas as suas vantagens.

Exemplos de funcionalidades:

- **Chamadas de vídeo**

As chamadas de vídeo, à semelhança das videoconferências, permitem ao emissor e ao receptor comunicar face-a-face em tempo quase real.

- **Bluetooth**

O Bluetooth é um sistema de captação de sinal wireless (sem fios) para dispositivos periféricos (por exemplo, impressoras ou ratos). Um telemóvel de Terceira Geração também pode vir equipado com tecnologia Bluetooth, permitindo a transferência de dados entre equipamentos activados para tal.

Com a tecnologia Bluetooth é possível, por exemplo, enviar fotografias ou mensagens de um telemóvel para outro, sem custos, desde que ambos estejam ao alcance da rede um do outro.

- **Acesso à Internet**

Uma das novidades dos telemóveis de Terceira Geração é poderem (quando equipados para tal) aceder à Internet. Tal como um computador, um telemóvel poderá aceder ao e-mail, aos chats e a outros sítios da Internet.

O acesso à Internet permite, por exemplo, carregar/descarregar as nossas imagens do telemóvel directamente para um blogue. Da mesma forma, também podemos descarregar ficheiros, como música ou fundos de ecrã.

Contudo, à utilização do telemóvel podem estar associados riscos. Por telemóvel pode receber vírus ou ser mais um meio de cyberbullying.

[Slide 11]

Um telemóvel, tal como os computadores, também é vulnerável a certos perigos, como os do phishing, SPAM, roubo de identidade e cyberbullying, pelo que algumas das regras que se aplicam para os primeiros aplicam-se aqui também.

- **Câmaras fotográficas**

A câmara fotográfica não constitui, por si, um perigo, mas a utilização por parte de indivíduos menos bem intencionados já o pode ser.

Se alguém tirar uma fotografia a uma pessoa sem a sua autorização (por exemplo, nuns balneários) e a colocar na Internet, isto constitui um acto de cyberbullying.

- **Cyberbullying**

O cyberbullying aplica-se aos telemóveis também, na medida em que é também possível receber uma mensagem (SMS), imagem (MMS), além de chamadas, cujo propósito seja o de intimidar, incomodar e/ou ameaçar, entre outros.

- **SPAM**

Embora não seja, por si só, um perigo, o SPAM (mensagens de texto ou outras contendo informação/publicidade não solicitada) pode ser extremamente incomodativo, na medida em que podemos receber inúmeros SMS que não nos interessam, a diversas horas do dia.

Contudo, tenha em atenção que o SPAM também pode conter phishing, pelo que deverá tratar estas mensagens com cuidado e reserva.

- **Bluetooth**

O Bluetooth pode, se o utilizador não for cuidadoso, ser um meio de invasão da privacidade. Se deixar o Bluetooth ligado, é possível a terceiros aceder sem autorização às informações do seu telemóvel. Para evitar que isto aconteça, desligue esta funcionalidade depois de efectuar a transferência de dados.

- **Vírus**

Embora seja ainda pouco comum receber vírus no telemóvel, este perigo existe e terá tendência, a par das outras tecnologias da comunicação, a crescer com o tempo. Hoje em dia, é possível alguém mal intencionado apagar remotamente dados de um telemóvel, desde que possua alguns dados a respeito do mesmo (nº de identificação, por exemplo).

Os vírus já se propagam nos computadores de bolso ("palmtops") e nos PDAs, pelo que é recomendável que tenha algum cuidado a transferir dados com esses equipamentos.

[Slide 12]

Algumas regras básicas que pode seguir para ter o seu telemóvel em segurança:

- **Evite dar o seu contacto telefónico a desconhecidos**

O seu número de telemóvel constitui um contacto directo consigo. Como tal, trate essa informação com o mesmo cuidado com que faria para a sua morada ou outros dados pessoais.

Há empresas que recolhem os dados pessoais dos clientes e as vendem a terceiros, podendo isso constituir um veículo para SPAM. Certifique-se que as empresas para as quais fornece os seus dados não tem essa política, lendo cuidadosamente as suas políticas de privacidade.

Da mesma forma, evite veicular o seu número de telemóvel através da Internet, pois pode ser interceptada por indivíduos menos bem intencionados e usada para fins ilícitos.

- **Não responda a mensagens cujo remetente é desconhecido**

Se não sabe de quem vem a mensagem e o seu conteúdo é desconfortável, não responda. Muitos cyberbullies e spammers desistem ao fim de algum tempo quando não obtêm resposta.

Se a mensagem for ameaçadora, reporte-a à polícia, anotando o remetente, a hora do envio e o seu conteúdo.

- **Evite atender chamadas não identificadas**

Da mesma forma que é imprudente responder a mensagens de números desconhecidos, as chamadas de número oculto também podem vir de entidades menos idóneas. Se quem está a ligar for alguém em quem confie, irá certamente deixar mensagem.

Esta regra é muito importante quando o telemóvel é de um adolescente ou criança, na medida em que estes são mais susceptíveis de ser aliciados para esquemas de publicidade enganosa e, no pior dos casos, sedução por parte de pedófilos.

- **Telemóveis nas mãos dos jovens**

O telemóvel tornou-se uma ferramenta essencial no dia-a-dia dos portugueses. Tendo-se tornado, um pouco por todo o lado, um objecto comum, também foi largamente adoptado pelos mais novos.

Estima-se que cerca de 80% dos jovens da Europa sejam proprietários de telemóveis. Como tal, cabe aos pais e educadores certificarem-se que algumas regras de segurança são cumpridas, para evitar colocá-los em riscos desnecessários.

Além das regras acima apresentadas, que devem ser cumpridas por todos, enumeramos aqui outras regras, dirigidas aos mais novos:

- **Os SMS são o passo seguinte depois dos chats**

É preciso recordar que os chats podem ser usados por indivíduos mal intencionados. Um pedófilo que esteja a tentar seduzir uma criança tentará obter o seu contacto telefónico, para enviar SMS e estar “presente” mesmo quando ela estiver longe da Internet. Esta é, a par com o envio de correio electrónico, uma das técnicas de sedução mais utilizadas pelos molestadores.

- **Não ter o telemóvel sempre à vista de todos**

É importante não tornar o jovem um alvo preferencial de furtos e/ou roubos. Ensinar aos mais novos a importância da discrição quando se usa um telemóvel em locais públicos é o primeiro passo para evitar alguns problemas.

- **Não andar e mandar mensagens ao mesmo tempo**

Embora pareça uma tarefa fácil, estar atento ao caminho e escrever mensagens de texto pode revelar-se perigoso, tal como demonstram os acidentes com jovens ao atravessar a rua.

- **Tarifário e registo de chamadas**

É importante o jovem saber qual o tarifário mais adequado ao seu uso de telemóvel e quanto gasta em média, para evitar fazer despesas excessivas. Uma regra de segurança importante é manter sempre o telemóvel com dinheiro suficiente para poder efectuar uma chamada, pois nem sempre uma situação exige o 112, mas pode pedir a ajuda dos pais (uma boleia de madrugada, por exemplo).

- **Comunicar é importante**

Por último, é de sublinhar que a comunicação entre os jovens e os seus encarregados de educação é um factor crucial para evitar situações de ocultação de informação – um adolescente deverá saber que pode contar com o educador caso se veja numa situação incómoda, e que juntos tentarão chegar a uma solução.

c. Vírus

[Slide 13]

Um vírus de computador é um programa informático que tem como propósito infectar o computador, fazendo com que o seu sistema operativo fique corrompido.

O vírus ataca agregando-se a um determinado programa já instalado no computador, de forma a que, quando este arranca, o vírus arranca com ele, propagando uma infecção. Este fenómeno ocorre, normalmente, sem o conhecimento do utilizador. Ao infectar o sistema operativo, um vírus poderá replicar-se a si mesmo e tentar infectar outros computadores, através de diversos meios.

Um vírus tanto pode ser um inofensivo programa que pouco mais faz que incomodar ligeiramente, como pode ir ao extremo de destruir ficheiros e tornar um computador inoperável. Contudo, uma característica comum a todos os vírus é a velocidade com que se propagam, contaminando outros ficheiros e computadores ligados à Internet que se revelem mais vulneráveis.

Uma das formas mais comuns de transmissão de vírus é através do e-mail. Há programas virais que se propagam de máquina em máquina através do uso das moradas de correio electrónico que figuram na lista do utilizador infectado. Outro método usado é pelo envio de uma mensagem de correio electrónico que, por exemplo, prometa prémios caso o cibernauta descarregue o ficheiro que se encontra nessa mensagem.

Outras formas de infecção podem incluir o download acidental de programas maliciosos que se encontrem “escondidos” dentro de outros programas, ou clicando em determinadas áreas de certos sítios de Internet menos bem intencionados.

A segunda maior causa de infecção deve-se ao facto de o utilizador não manter o seu sistema operativo actualizado, com a instalação dos “patches” (“remendos”) que o fabricante vai disponibilizando à medida que vai detectando falhas.

Apresentamos de seguida algumas técnicas de “auto-preservação” dos vírus:

- **Ocultação nas pastas do sistema**

Dado que uma grande parte dos utilizadores de computadores não possui conhecimentos especializados em informática, os vírus implantam-se no sistema operativo, a fim de evitar que o utilizador comum tente removê-los. Esta técnica acaba por ser dissuasora, porque o utilizador médio terá receio de remover ficheiros do sistema, corrompendo o normal funcionamento do seu sistema.

- **Encriptação**

Os vírus “escondem-se” encriptando os seus próprios dados: assim, o seu código será mais dificilmente detectado pelos antivírus e será mais difícil a sua remoção, embora cada vez mais os antivírus estejam melhor preparados para esta técnica. O propósito desta técnica é manter a infecção o maior tempo possível no computador.

- **Tentativas de desactivar o antivírus**

Esta é a melhor forma de evitar a detecção e remoção de vírus.

[Slide 14]

Um vírus de computador está programado para se esconder da melhor forma possível, para evitar a sua detecção e remoção.

Uma infecção por vírus pode trazer sérias consequências para o proprietário do material infectado, pois corrompe ficheiros, podendo até inutilizá-los, torna o sistema operativo muito mais lento e, em ocasiões, pode até usurpar os dados pessoais do utilizador.

Para saber mais acerca dos malefícios dos vírus, consulte as secções correio electrónico, Peer-to-Peer e phishing.

[Slide 15]

- **Tenha o antivírus actualizado**

Embora não seja infalível, um antivírus ajuda-o evitar que muitos vírus infectem o seu computador.

- **Não abra ficheiros de origem suspeita**

Os ficheiros enviados por correio electrónico, mesmo de origem conhecida, podem conter material malicioso. Corra-os primeiro com o antivírus. Se forem de origem desconhecida ou desconfiar de phishing, não abra esses ficheiros.

- **Tenha o seu sistema operativo actualizado**

O seu fornecedor de sistema operativo actualizará, de forma gratuita, no seu sítio de Internet, os chamados “patches” (“remendos”) para corrigir eventuais fragilidades que possam facilitar a entrada de programas maliciosos. Tenha sempre o seu computador actualizado.

- **Tenha a firewall sempre activa**

Uma firewall é uma protecção adicional contra a entrada de programas indesejados no seu computador, pelo que a deverá ter sempre activa e actualizada.

d. Redes Sociais Virtuais

[Slide 16]

Enquanto seres sociais, os seres humanos procuram constantemente interagir com outros, nas mais diversas ocasiões. Esta realidade também se aplica ao mundo da Internet, tanto mais que esta permite que as pessoas comuniquem umas com as outras de qualquer parte do mundo.

Uma rede social virtual é, portanto, um reflexo dessa necessidade de comunicar, aplicado às redes Web. É deste modo que o sujeito se apresenta aos restantes internautas, quer seja através de páginas pessoais ou através de blogues, mostrando-se ao mundo dos mais diversos modos: por fotografias, pela escrita, por vídeos.

O objectivo de uma rede social virtual é permitir ao utilizador expressar-se de um modo pessoal e contactar com outros indivíduos que partilhem interesses semelhantes. Assim, os sítios Web destinados à interacção social virtual estão especificamente desenhados para os utilizadores partilharem informações acerca de si (tais como a idade, data de nascimento, os filmes e livros favoritos, opiniões, entre outros) e convidam, na sua grande maioria, ao envolvimento de terceiros, através da possibilidade de comentar os diversos elementos colocados nessa página pessoal.

Embora os blogues também sejam uma expressão das redes sociais virtuais, optámos por remetê-los para uma secção própria, focando-nos aqui apenas nas páginas de perfil pessoal que, um pouco por todo o mundo, os utilizadores escolhem criar de para se apresentarem aos outros internautas.

Para poder aceder às funcionalidades de uma rede social virtual, o utilizador apenas tem que se inscrever num sítio Web que ofereça esse serviço. A maioria (e os mais populares) dos sítios fornece este serviço de forma gratuita.

São pedidos dados pessoais no acto de inscrição, alguns dos quais serão visíveis aos outros utilizadores. Os dados partilhados são vistos como uma forma de apresentação online, permitindo aos interessados procurar afinidades com aquele utilizador e, eventualmente, solicitar que esse figure na rua “rede de amigos”.

Dado que o propósito de uma rede social virtual é fomentar a interacção entre os vários utilizadores que também acedem a essa rede, cada página pessoal é regida pelo princípio dos “amigos em rede,” ou seja, espera-se que cada utilizador recém-inscrito adicione como seus amigos online todas as pessoas inscritas que já conhece no mundo real, ficando assim ligado aos amigos desse amigo de forma indirecta. Esses amigos, por sua vez, ao aceder à página pessoal do utilizador que já conhecem, verão o recém-inscrito e poderão fazer-lhe um pedido de adição que, caso seja aceite, fará com que essa pessoa passe a ser também “amigo” de quem fez o pedido.

O valor da rede social virtual de cada utilizador está exponencialmente ligado ao número de pessoas que se encontram nessa rede. Como se pode verificar, a designação de “amigo” nas redes sociais é usada de forma bastante alargada, pois basta que um utilizador aceite um pedido de amizade (“friend request”) de outro indivíduo para que este figure na sua “lista de amigos”.

A lista de amigos virtuais de uma pessoa é considerada, por muitos, um espelho da sua popularidade online. Há quem considere tanto mais popular quanto mais “amigos” tiver nessa lista. Uma das actividades mais praticadas pelos internautas nas redes sociais virtuais é navegar pelos perfis à procura de pessoas com um determinado perfil para lhes enviar pedidos de amizade e, assim, estabelecer algum tipo de contacto com elas.

As páginas de redes sociais oferecem também, geralmente, uma série de outras funcionalidades que facilitam a comunicação com os demais: o utilizador pode colocar músicas no seu perfil que são ouvidas por aqueles que acederem à sua página, escrever artigos na secção do seu blogue, colocar fotografias na sua galeria, enviar e receber mensagens privadas, tudo em nome da interacção social virtual.

Além da sua página pessoal, o internauta é convidado a navegar pelos perfis dos outros utilizadores e comentar os conteúdos colocados nos mesmos, estabelecendo assim uma comunicação com eles. As regras de etiqueta do mundo real também se aplicam no mundo virtual, e é esperado que haja reciprocidade de comentários.

Os meios de promoção de celebridades ou aspirantes a tais não são alheios ao mundo das redes sociais virtuais, sendo frequente os artistas dos mais diversos ramos procurarem mostrar-se recorrendo a estas redes. Os fornecedores das mesmas, conhecendo as potencialidades deste tipo de promoção, fornecem, muitas vezes, páginas de perfil próprias para este tipo de clientes. No caso de celebridades francamente notórias, é frequente as páginas serem geridas por indivíduos contratados para tal.

[Slide 17]

As redes sociais virtuais são uma forma bastante popular de estabelecer contacto com outros indivíduos que, caso contrário, o utilizador poderia nunca vir a conhecer. Contudo, como qualquer serviço fornecido através da Internet, apresenta variados perigos, que vamos referir de seguida.

- **Dados pessoais na página de perfil**

Dado que o objectivo é apresentar-nos aos demais, uma página de perfil terá, necessariamente, dados pessoais acerca do seu criador. É natural referirmos os nossos filmes favoritos, os livros que mais nos marcaram, até o nosso desporto favorito. No fundo, colocamos todas as informações que consideramos relevantes, para assim podermos encontrar outros utilizadores com gostos semelhantes.

Contudo, há dados que podem representar um perigo se forem partilhados, em especial se o utilizador for um menor. Referir a cidade onde vive ou a escola que frequenta é abrir as portas aos predadores online, que procuram activamente formas de contactar pessoalmente as suas potenciais vítimas.

Este perigo não se aplica somente aos mais novos: lembre-se que, por exemplo, referir os seus rendimentos anuais é convidar sujeitos mal-intencionados a tentar explorá-lo. Se, além dos rendimentos, referir também a sua localidade, o trabalho destes criminosos está altamente facilitado.

- **Apropriação de identidade**

Dada a popularidade das redes sociais virtuais, estas tornaram-se também um local onde os criminosos virtuais tentam enganar os utilizadores menos atentos. Uma forma de o conseguir é entrando de forma ilícita no perfil dos utilizadores dessas redes e, através destas, enviar mensagens aos amigos da lista da vítima com mensagens de publicidade, phishing, SPAM e outras comunicações não solicitadas.

Muitas vezes, os legítimos proprietários das páginas pessoais não se dão conta deste facto, podendo ser depois alvo de manifestações de desagrado por parte de quem recebeu as mensagens.

Além dos propósitos publicitários e/ou de recolha ilegítima de dados, também há a apropriação que apenas pretende incomodar o utilizador: um método recorrente é o de enviar mensagens na forma de boletins (vistos por todos os amigos na lista dessa pessoa) com frases obscenas ou convites explícitos para as mais diversas actividades. Este fenómeno pode ser visto como uma forma de cyberbullying.

- **Falsas identidades**

Tendo em conta a facilidade com que se pode criar uma página pessoal nos sítios de redes sociais virtuais, um utilizador mal-intencionado também pode criar uma página com dados falsos para atrair um determinado tipo de pessoas e as enganar, importunar ou explorar. Um exemplo disso são os molestadores de crianças, que criam páginas de perfil fazendo-se passar por jovens com determinados interesses, a fim de se aproximarem de uma criança vulnerável.

- **Imagens, opiniões e outros.**

É muito fácil um utilizador perder o controlo dos dados que coloca na sua página pessoal: assim que um dado fica online, muito dificilmente desaparecerá, mesmo se depois for apagado. É muito fácil, por exemplo, alguém copiar as imagens colocadas num perfil e divulgá-las por outros, distorcê-las e até inseri-las noutras situações, descontextualizando-as completamente.

Uma opinião manifestada de determinada forma numa página pessoal pode inflamar os ânimos de outro utilizador e, assim, gerar uma onda de insultos. Reportando-nos novamente às imagens, as fotografias de conteúdo provocante também podem suscitar reacções indesejadas e/ou perseguições online e na vida real.

Por outro lado, já é frequente alguns empregadores pesquisarem as informações colocadas online por parte dos candidatos a determinados empregos, a fim de verificar se o perfil destas se adequa ao que a empresa pretende. Da mesma forma, também são conhecidos os casos de funcionários que são despedidos por manifestarem determinadas opiniões acerca dos seus empregadores nas suas páginas de rede social ou blogues.

- **Cyberbullying**

Embora já nos tenhamos referido a este factor nos outros pontos desta secção, é importante sublinhar a sua existência. O cyberbullying não é alheio às redes sociais virtuais, dado que é precisamente nestas redes que os utilizadores se tendem a expor mais.

Alguns sítios de redes sociais dão aos utilizadores a possibilidade de classificar cada perfil numa dada escala (por exemplo, de “morno” a “quente!”). Embora possa parecer inócua, esta funcionalidade pode fomentar a discriminação dos utilizadores com base nas suas características, como as raciais, de orientação sexual ou aparência física. Incentivar outros a dar uma classificação negativa e enviar comentários de ataque à dignidade do utilizador são formas de cyberbullying.

- **Ausência de controlo efectivo de idade**

Embora os sítios de redes sociais virtuais definam uma idade mínima permitida para se ter uma página pessoal, nada impede um jovem com idade inferior ao permitido de se inscrever na mesma. A ausência de métodos de controlo eficazes faz com que um jovem de reduzida idade possa ser exposto a conteúdos inapropriados ou, de modo ainda mais preocupante, ser abordado por pessoas que, sabendo ou não a sua idade real, o possam lesar de alguma forma.

- **(Quase) ausência de moderação**

Embora tenha pessoas especializadas encarregues de monitorizar os conteúdos das páginas pessoais, os sítios Web das redes sociais virtuais possuem demasiados utilizadores para o número de moderadores existente, facilitando assim a inserção e manutenção de conteúdos que vão contra as regras de funcionamento dos sítios. É esperado que os utilizadores se monitorizem uns aos outros, reportando aos moderadores a existência de conteúdos inapropriados nos perfis visitados.

Por outro lado, mesmo quando há reporte de conteúdos inapropriados, e os mesmos são retirados, é complicado vigiar esse perfil e ver se estes são novamente colocados online. Quando uma conta é cancelada, torna-se igualmente complicado barrar o acesso desse utilizador a um sítio Web gratuito – nada o impede, portanto, de abrir nova conta e inserir dados diferentes, usufruindo impunemente da sua nova conta.

[Slide 18]

Dada a popularidade das redes sociais virtuais, torna-se de extrema importância que o utilizador conheça as formas de se proteger contra possíveis ameaças.

- **Não forneça inadvertidamente dados pessoais**

Evite colocar informações que possam levar desconhecidos a encontrá-lo(a), como por exemplo dados sobre o local onde reside, trabalha, números de telefone. Esta regra é tanto mais importante quanto mais jovem for o utilizador: informe os seus educandos acerca dos perigos de colocar informação pessoal online e explique-lhes porque nunca deve escrever algo que possa levar alguém a identificá-lo e encontrá-lo.

- **Não aceite pedidos de amizade se o conteúdo da página o deixar desconfortável**

Se receber um pedido de amizade na sua página pessoal, veja sempre a página dessa pessoa. Leia o que essa pessoa escreve, veja as suas fotografias e leia os comentários deixados por outros utilizadores. Se houver alguma coisa que o deixe desconfortável, recuse adicionar essa pessoa à sua lista. Um pedido é isso mesmo, e cabe a quem o recebe decidir se o quer aceitar ou não.

Lembre-se que, em caso de dúvida, o melhor é recusar um pedido. Aceitar figurar como “amigo(a)” de outro utilizador é uma forma implícita de mostrar concordância com os seus ideais e pensamentos. Se um perfil contiver dados que vão contra a sua forma de pensar, quer ser associado(a) ao autor dos mesmos?

- **Não responda a comentários ou conteúdos ofensivos**

Se alguém colocar um comentário ofensivo no seu perfil, opte por apagar esse comentário e a pessoa que o fez da sua lista de amigos. Certifique-se, no entanto, que a mensagem não adveio de uma apropriação indevida de identidade, caso contrário, estará a eliminar alguém inocente.

Caso o comentário ou conteúdo enviado vier legitimamente desse utilizador e o mesmo for contra as regras do sítio Web, reporte-o aos moderadores.

- **Os dados não são privados**

A regra de ouro é: tudo o que for colocado na Internet deixa de ser privado. Mesmo que o seu perfil esteja definido como privado, nada impede a quem tenha acesso autorizado ao mesmo de copiar os seus conteúdos e enviá-los a terceiros. Se pensar em colocar algo na sua página pessoal que o deixe com dúvidas, opte por não o colocar de todo.

e. Chats e IMs

[Slide 19]

- **O que é um chat?**

Um chat (abreviatura de “chatroom”, ou “sala de conversação”, em português) é um local online destinado a juntar várias pessoas para conversarem. Este local pode ser de índole generalista, ou pode destinar-se à discussão de um tema em particular (por exemplo, um chat sobre ecologia).

Os chatrooms permitem que várias pessoas troquem opiniões por escrito em simultâneo, em tempo real. Quando um utilizador escreve algo no chatroom, as suas palavras ficam disponíveis no painel para todos lerem, dando assim oportunidade aos restantes elementos presentes de responder da mesma forma.

- **O que é um IM?**

Um IM (ou “Instant Messaging”, ou “mensagens instantâneas”, em português) é uma forma fácil de manter contacto com alguém sem ter que esperar por um e-mail. Alguns exemplos de IMs são o MSN Messenger, o Google Talk, o Yahoo! Messenger e o Skype, sendo que este último privilegia a utilização da voz como meio de comunicação.

Os IMs são muito utilizados para manter contactos lúdicos e informais, sendo também uma plataforma comum para a troca de informação por funcionários de empresas, enquanto ferramenta de trabalho. Para tal, basta que as pessoas envolvidas se encontrem online.

Este método de conversação via Internet é cada vez mais utilizada por jovens para conversar com os seus pares ou conhecer gente nova. Dadas as suas características (ser uma forma de contacto que não decorre frente-a-frente), muitos jovens sentem-se protegidos e, confiando em desconhecidos, podem discutir assuntos ou partilhar informação com mais à-vontade do que se fosse “ao vivo”.

- **Como funciona um Chat?**

Cada chat tem o seu conjunto de regras particulares, as quais se espera que sejam respeitadas (por exemplo, não ser permitido falar de música nos tópicos de ecologia). Para assegurar que tal acontece, alguns chats têm a presença de um moderador, que é uma pessoa responsável pelas actividades/temas/utilizadores que se encontram nesse local cibernético. Cabe ao moderador manter o bom funcionamento da “sala de conversa”, podendo expulsar aqueles que considere estarem a agir de modo impróprio. É ao moderador que deve reportar alguma ocorrência que sinta ser incorrecta.

Um dado importante a reter é que, apesar de, nestes chats, as conversas serem públicas, há também a possibilidade de se conversar em privado (“private chats”) com terceiros. Estas conversas já não são moderadas e, conseqüentemente, podem apresentar alguns perigos, sobretudo para os cibernautas mais jovens (por exemplo, um menor pode, inadvertidamente, conversar com um pedófilo, ou com alguém que se queira apropriar da sua identidade ou da dos seus familiares, ou até obter informações que lhe permitam planejar um roubo).

- **Como funciona um IM?**

O sistema de mensagens instantâneas junta as funcionalidades do chat, dos telefones e do e-mail e permite a troca de informação e dados de forma quase imediata, a todos os utilizadores na lista de amigos desse utilizador que se encontrem online.

Para tal, basta que escrevamos a mensagem, cliquemos em “enviar” e a mensagem é recebida quase instantaneamente pelo destinatário, onde quer que se encontre. É possível trocar mensagens instantâneas por computador, telemóvel ou por outro meio que possua ligação à Internet. Um telemóvel pode receber uma mensagem instantânea vinda de um computador e vice-versa.

Há programas de IM que permitem ao cibernauta comunicar além da forma escrita, recorrendo à voz, ao vídeo ou às imagens, desde que possua as ferramentas necessárias (um microfone, ou uma webcam, por exemplo).

[Slide 20]

Os chats e os IMs podem ser locais perigosos para crianças e jovens, dado nunca termos a certeza de quem é o cibernauta que se encontra do outro lado. Os chatrooms são um local privilegiado para os pedófilos angariarem crianças desprevenidas, pelo que é importante preparar e educar os mais novos acerca dos potenciais perigos deste meio.

Outro fenómeno ao qual devemos estar atentos é o do cyberbullying, que consiste em ameaçar, insultar ou denegrir uma pessoa através das mais variadas técnicas.

Um chat ou um IM pode ser o local escolhido por certos indivíduos para cometerem alguns crimes, tais como o roubo de identidade e fraude.

[Slide 21]

Algumas sugestões para uma utilização segura dos chats e IMs.

- **Tenha atenção aos temas explorados num chatroom**

Os assuntos discutidos num chat dizem muito acerca dos seus utilizadores. Se não se sentir confortável com os temas abordados, o mais certo é também se sentir desconfortável com as pessoas que lá se encontram. Se for esse o caso, opte por sair do chat e explique ao seu filho que o deve fazer caso o mesmo lhe suceda.

- **Escolha um nome de utilizador (username) que não revele informação pessoal e incentive o seu filho a fazer o mesmo**

Ter um nome de utilizador que indique o seu sexo, idade, ocupação ou local de residência é um chamariz para aqueles que procuram os chats com intenções que podem não ser do seu agrado. Certifique-se também que os seus filhos não divulgam este tipo de informação no seu username.

- **Evite preencher o campo dos dados no perfil**

Alguns serviços de mensagens instantâneas e chats encorajam o cibernauta a colocar um “perfil” com informação variada, tal como idade, sexo, ocupação ou interesses de tempos-livres. Embora estes dados permitam ao utilizador conhecer outras pessoas com interesses semelhantes, podem também torná-lo vulnerável a certos ataques. Dado que estas informações podem ser transferidas pela empresa de IM para um directório, é conveniente que aconselhe os seus filhos a não preencher esse campo, por torná-los mais vulneráveis a predadores.

- **Não divulgue informação privada a desconhecidos nem deixe os seus filhos fazê-lo**

Tenha sempre em mente que, por mais que julgue conhecer uma pessoa com quem falou online, essa pessoa não deixa de ser, essencialmente, um estranho. Como tal, use o bom-senso e não divulgue informação pessoal ou envie fotografias. Lembre-se que esta informação pode ser reenviada para fins com os quais não concorde.

As crianças e jovens que utilizam a Internet, por serem mais ingénuas, são essencialmente um alvo fácil para certos tipos de pessoas. Tenha em mente que este é um meio usado por molestadores de crianças para as seduzir, e o primeiro passo é aliciá-las a fornecer dados privados, vulnerabilizando-as.

- **Não aceite encontrar-se com desconhecidos e não deixe os seus filhos fazerem-no**

Uma das características da Internet é o seu relativo anonimato. Como tal, um homem de 40 anos pode fazer passar-se por uma criança de 12 e ser bem sucedido – isto quer dizer, no fundo, que nunca podemos ter a certeza de que estamos a falar com alguém confiável e honesto. Seja precavido e não aceite encontrar-se com alguém que não conheça já pessoalmente, nem deixe que os seus filhos o façam.

- **Não abra ficheiros nem aceda a páginas de Internet enviadas por desconhecidos**

Se alguém que não conhece lhe enviar um ficheiro, não o abra (ou, se tiver mesmo que o fazer, corra um antivírus nesse ficheiro antes). Este pode conter um vírus informático, que lhe infectará o computador, afectando o seu funcionamento. Da mesma forma, não aceda a links que lhe sejam transmitidos sobre os quais tenha dúvidas, pois pode tratar-se de uma forma de phishing.

- **Registe as sessões de conversação**

A maior parte das aplicações de chat ou IM permitem ao utilizador gravar as conversas que tem com os vários participantes. Opte por activar esta funcionalidade, pois poder-lhe-á ser útil caso as coisas se compliquem. Certifique-se que os seus filhos também guardam as conversas que têm online. Este tipo de registo já se provou útil para o decurso de investigações a predadores na Internet.

f. Peer-to-Peer

[Slide 22]

O Peer-to-Peer, ou P2P (“de parceiro para parceiro,” numa tradução livre), é um sistema que permite a um utilizador trocar e partilhar ficheiros com outros utilizadores de forma directa, isto é, sem um sítio de Internet ou outro sistema centralizado. O facto de essa troca ser feita de um computador para outro, sem “intermediários”, é o que faz a esta funcionalidade merecer a sua nomenclatura.

Existem vários serviços de P2P disponíveis para serem descarregados na Internet, e a grande maioria é utilizada para a partilha de ficheiros de vídeo, áudio, programas e software.

Os P2P têm sido alvo de algumas críticas por parte de diversas entidades, por se considerar que, ao permitir a partilha de certos dados, tais como músicas e filmes, estes poderão estar a violar certos direitos de autor e a fomentar a pirataria.

Para poder utilizar um Peer-to-Peer, o cibernauta terá que proceder à instalação de um software apropriado. Existem vários disponíveis para serem descarregados na Internet, tendo cada um deles o seu sistema de funcionamento próprio.

Uma característica de uma rede P2P é a mutabilidade de papéis de um computador (ou outro tipo de unidade de processamento), passando de cliente a servidor e de servidor a cliente, conforme se encontra a descarregar ficheiros, ou a partilhá-los, respectivamente.

Ao instalar um serviço de P2P, o utilizador está a permitir que outros cibernautas tenham acesso a uma determinada pasta de conteúdos (escolhida por si) e possam, conseqüentemente, consultá-la e retirar de lá os ficheiros que considerem interessantes. Assim sendo, terá que ter em conta que, para efeitos de funcionamento, essa pasta será considerada “de acesso livre” aos restantes cibernautas que utilizem esse P2P.

[Slide 23]

- **Violação dos direitos de autor**

Ao instalar um P2P no seu computador, terá que ter em conta que é possível que vá encontrar material para descarregar, tal como filmes, software ou álbuns de música, pelos quais não está a pagar quaisquer direitos de autor. Isto constitui uma ilegalidade e é a principal crítica efectuada a este tipo de serviço de partilha de dados.

- **Propagação de vírus**

O P2P também é uma forma utilizada pelos piratas da Internet para infectar outros computadores, distribuindo vírus em ficheiros aparentemente inocentes. Uma vez dentro do computador, o vírus poderá afectar o funcionamento do seu computador, corromper dados e até apropriar-se dos seus dados pessoais, tais como palavras-passe.

- **Ficheiros falsos**

Tal como foi referido, nem sempre um ficheiro é aquilo que aparenta – por exemplo, um cibernauta pode pensar que está a descarregar uma fotografia de uma celebridade e, quando abre o ficheiro recebido, constata que recebeu material pornográfico. Isto pode causar alguns incómodos, nomeadamente, se o P2P é usado por um menor.

- **Partilha de dados altamente lesivos**

Dado o relativo anonimato dos indivíduos inscritos num serviço P2P (cada utilizador possui um nickname, que o identifica, não precisando de usar o seu nome real), este é um meio conhecido de os pedófilos partilharem material ilícito com menores.

- **Funcionalidades “extra”**

Por fim, tenha em atenção que é possível que algum do software usado para aceder a um serviço P2P pode conter algumas funcionalidades “extra” incómodas, tais como “spywares” ou “adwares”, que são programas que invadem o seu computador, inundam-no de publicidade indesejada e podem até aceder à sua informação pessoal.

[Slide 24]

- **Tipos de programas partilhados**

Antes de instalar um Peer-to-Peer, lembre-se que o mesmo pode autorizar (ou, no mínimo, não proibir) a troca ilegal de ficheiros com direitos de autor. Assim, pense bem se quer estar a participar numa actividade punida pela lei.

Antes de instalar um P2P num computador que não é seu, peça autorização. Evite instalar esta funcionalidade num computador do seu local de trabalho, pois estará a comprometer a segurança da sua empresa, em especial se a mesma tiver todos os seus computadores ligados em rede.

- **Verifique a qualidade do programa**

Antes de instalar um P2P, certifique-se que o mesmo é idóneo. Poderá aceder, mediante pesquisa na Internet, a sítios especializados que tenham a apreciação de outros cibernautas acerca do mesmo, contendo a sua opinião e comentários vários.

Da mesma forma, certifique-se que descarrega o programa que pretende de um sítio igualmente idóneo, para evitar instalar um programa com funcionalidades “extra”.

- **Saiba o que contém a sua pasta de partilha**

Verifique sempre os conteúdos das pastas às quais vai permitir o P2P aceder. Lembre-se que, uma vez definidas como pastas de partilha, as mesmas estarão ao inteiro dispor dos outros utilizadores. Como tal, é aconselhável que retire todo o tipo de informação pessoal que possa ter nesse local, tais como fotografias ou outros dados pessoais.

- **Corra sempre um antivírus**

Corra sempre um antivírus antes de abrir um ficheiro descarregado de um P2P. Não se esqueça que não sabe se o mesmo é, efectivamente, aquilo que o nome indica ser.

- **Vigie a utilização do P2P por parte dos seus educandos**

Como já foi referido, um ficheiro pode não ser o que diz ser. Imagine que o seu educando descarregou um programa apropriado para crianças e depois, ao corrê-lo, este é, na realidade, um ficheiro contendo pornografia.

Todo o cuidado é pouco e, no tocante a crianças, o melhor é vigiar de perto os conteúdos procurados pelo seu educando e abrir os mesmos antes, sem a presença dele, para evitar surpresas desagradáveis.

Tenha em mente que alguns Peer-to-Peer possuem a funcionalidade do chat incorporado no programa. Como tal, todas as informações de segurança relativas a este tipo de serviço devem ser tidas em conta aqui também.

g. Correio electrónico

[Slide 25]

O e-mail (abreviatura de “electronic mail”, ou correio electrónico, em português) consiste num meio de enviar mensagens escritas pela Internet e que tem a vantagem de ser recebido 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 passa pela possibilidade de o utilizador criar listas de distribuição de endereços de correio electrónico, podendo enviar uma mensagem para várias pessoas ao mesmo tempo.

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

- possuir uma ligação à Internet;
- estar registado num servidor de e-mails;
- escrever a sua mensagem, colocar o endereço electrónico 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 electrónico tem os seus perigos, como a propagação de vírus, devendo o utilizador tomar algumas precauções para assegurar ao máximo a protecção dos seus dados e do seu computador.

[Slide 26]

Tal como outras funcionalidades no mundo da Internet, também o correio electrónico pode apresentar os seus perigos. Um dos perigos mais comuns é a propagação de vírus e consequente infecção dos computadores de utilizadores domésticos e empresariais (veja também Phishing).

Os vírus são propagados de diversas formas, como por exemplo, através de mensagens não solicitadas de correio electrónico 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 encoraja o receptor a abri-lo.

A este tipo de técnica de encorajamento dá-se o nome de Engenharia Social (sendo disto um grande exemplo o phishing), que se serve da natureza crédula e curiosa para aliciar o cidadão menos atento.

Uma infecção por vírus pode ter consequências nefastas no seu sistema informático. Estas consequências incluem por exemplo:

- **Revelar informação**

Os vírus propagados por mensagens de correio electrónico em massa (SPAM) podem ter como principal objectivo a recolha de endereços de correio electrónico 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 infectados 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 electrónico 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).

[Slide 27]

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

- **Corra e mantenha uma aplicação antivírus 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 actualizada, ferramentas ou bases de dados de vírus para ajudar na detecção e recuperação de código malicioso. 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.

- **Mensagens que avisam de perigos (reais?)**

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 fazer o cibernauta reenviar aquela mensagem para o maior número de pessoas conhecidas e, assim, apropriarem-se de moradas de e-mail, que depois encham de SPAM.

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

- **Não corra programas de origem desconhecida**

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

Não descarregue, instale ou corra programas a menos que saiba que este é da autoria de uma pessoa ou companhia 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 também 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 utilizadores a visitar “web sites” maliciosos.

- **Não envie informação confidencial por e-mail**

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.

- **Use uma “firewall” pessoal**

As “firewalls” filtram portos e protocolos desnecessários de Internet, evitando ao utilizador correr 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.

- **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 afectar 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 electrónico permita, desligue o modo de visualização de e-mails em formato html**

h. Cyberbullyng

[Slide 28]

A expressão “cyberbullying” carece de tradução formal em português. É uma palavra composta, sendo o “cyber” relativo ao uso das novas tecnologias de comunicação (correio electrónico,

telemóveis, etc.) e o “bullying” relativo ao fenómeno dos maus-tratos por parte de um rufião (“bully”) ou grupo de rufiões.

O cyberbullying consiste no acto de, intencionalmente, uma criança ou adolescente, fazendo uso das novas tecnologias da informação, denegrir, ameaçar, humilhar ou executar outro qualquer acto mal-intencionado dirigido a outra criança ou adolescente.

Um cyberbully pode tornar-se, no momento seguinte, também ele uma vítima. É frequente os jovens envolvidos neste fenómeno mudarem de papel, sendo os maltratantes numa altura e as vítimas noutra.

Envolvendo três vectores (bully – vítima - novas tecnologias da informação e comunicação), o cyberbullying é um fenómeno em rápido crescimento, em particular no mundo da Internet.

Por ser um fenómeno que envolve crianças e adolescentes, com todas as sensibilidades e percursos desenvolvimentais cruciais próprios destas idades, carece de especial atenção por parte de todos os pais e educadores. Embora sejam, na sua maioria, eventos ultrapassáveis, algumas vítimas de bullying chegam a tentar o suicídio, provando que não devemos encarar tal situação de ânimo leve.

Quando a vitimização envolve adultos, passa a ter a designação de “cyber-harrassment” (“assédio cibernético”) ou “cyberstalking” (“perseguição cibernética”), tendo, contudo, as mesmas características. Por tal, as sugestões apresentadas servem também para estes casos.

Os métodos usados por um cyberbully são os mais variados. Com o advento das novas tecnologias de informação e comunicação (correio electrónico, telemóveis, etc.), o bully serve-se destas para transtornar a sua vítima, ameaçando-a, denegrindo a sua imagem, causando-lhe grande sofrimento e stresse, podendo até ter consequências fatais.

A crueldade não é alheia aos jovens e o que motiva os rufiões cibernéticos são as mais variadas razões, que vão desde o gozo de ver o outro a ser humilhado e atormentado, à vingança por também terem sido já alvos de cyberbullying.

Se, na escola, o maltratante era o rapaz ou rapariga em situação de maior poder (tamanho, idade ou outro), no mundo cibernético as regras “tradicionais” da rufiagem esbatem-se e o cyberbully pode ter os mais variados perfis.

Seguem-se alguns exemplos de cyberbullying:

- **Ameaças/perseguições**

Os cyberbullies servem-se do correio electrónico, do IM e dos telemóveis (via SMS) para enviar mensagens ameaçadoras ou de ódio aos seus alvos.

Os rufiões podem-se fazer passar por outras pessoas, adoptando usernames (nomes de utilizador) parecidos com os delas, para envolver outros inocentes no processo.

- **Roubo de identidade ou de palavras-passe**

Ao conseguir acesso ilícito às palavras-passe do seu alvo, o rufião serve-se delas para entrar nas variadas contas da vítima, causando os mais variados distúrbios:

- Por e-mail: envia mensagens de conteúdo obsceno, rude ou violentos em nome dela para a sua lista contactos;
- Por IM ou em chats: difunde boatos, faz-se passar pela vítima e ofende as pessoas com quem fala;

Entrando nos sítios de Internet nos quais a vítima tem um perfil inserido, por exemplo, para conhecer pessoas novas: altera o perfil de utilizador dessa conta (incluindo, por exemplo, comentários de

natureza racista, alterando o sexo do utilizador ou inserindo itens que possam difamar a imagem do utilizador legítimo da conta), ofendendo terceiros e atraindo a atenção de pessoas indesejadas.

O rufião pode depois alterar as palavras-passe das variadas contas, bloqueando assim ao seu legítimo proprietário o acesso às mesmas.

- **Criação de páginas de perfil falsas**

O jovem mal-intencionado cria uma página pessoal na Internet acerca do alvo dos seus ataques, sem o conhecimento deste, na qual insere todo o tipo de informações maldosas, trocistas ou falsas, além de poder conter dados reais, como a morada da vítima. Seguidamente, faz chegar a terceiros a morada desta página, para que o maior número de pessoas a veja. Este tipo de difusão de informação pode, por vezes, ter as características de uma epidemia, espalhando-se rapidamente pelos cibernautas.

Esta atitude pode ter consequências perigosas, dado poder informar outros utilizadores menos bem intencionados (por exemplo, um pedófilo) onde poderá encontrar este jovem na vida real, colocando a sua vida em potencial risco.

- **O uso dos blogues**

Um blogue consiste numa espécie de diário online, na qual o utilizador escreve os mais variados artigos. Embora tenha o propósito original de partilhar informações com outros cibernautas, há cyberbullies que se servem dos blogues para difundir dados lesivos a respeito de outras pessoas, seja escrevendo nos seus blogues pessoais, seja criando blogues em nome das suas vítimas.

- **Envio de imagens pelos mais variados meios**

O rufião envia mensagens de correio electrónico em massa para outros cibernautas, contendo imagens degradantes dos seus alvos. Estas imagens podem ser reais ou montagens, e podem difundir-se rapidamente, humilhando e lesando grandemente a imagem da vítima.

Outra forma de envio é por telemóvel. Com o advento dos telemóveis que permitem tirar fotografias, é possível fotografar uma pessoa sem que ela se dê conta e difundi-la pelos amigos. Um grande exemplo disto são as fotografias tiradas subrepticiamente pelo adolescente aquando de uma relação sexual ou encontro mais íntimo, havendo já relatos destes acontecimentos em Portugal. Estas imagens, além de serem difundidas por telemóvel, podem ser descarregadas para a Internet, alcançando ainda mais pessoas.

- **Sítios de votação**

Existindo variados sítios de Internet onde se pode votar acerca dos mais variados assuntos, é possível a um jovem criar o tema de “A Mais Impopular”, “O Mais Gordo”, etc., visando quem deseja incomodar.

- **Envio de vírus**

Não se pense que o envio de vírus é exclusivo dos adultos. Com a crescente precocidade dos cibernautas mais jovens, uma forma de prejudicar os seus pares pode ser enviar-lhes vírus para lhes infectar o computador, roubar palavras-passe (veja “Roubo de identidade ou de palavras-passe”, mais acima) e causar incómodos.

- **Inscrições em nome da vítima**

É perfeitamente possível um cibernauta inscrever-se num determinado sítio de Internet usando os dados de outra pessoa. Os locais escolhidos costumam ser sítios de pornografia, fóruns racistas ou outros que sejam contrários à ideologia da vítima. O resultado disto é esta ser “inundada” de e-mails que não são do seu interesse, podendo os mesmos até ser nocivos.

[Slide 29]

Muitas vezes estes ataques são perpetrados por jovens contra outros jovens. Dadas as características próprias desta etapa desenvolvimental, já por si marcada pelo advento de tantas mudanças sensíveis, o bullying pode assumir contornos graves que levem as vítimas a situações altamente incómodas e indesejáveis.

Embora, na sua maioria, os actos de bullying não tenham consequências tão drásticas, podem, no entanto, causar igualmente um grande sofrimento, chegando a levar à depressão, à exclusão pelos pares, ao isolamento, ao desespero.

O rufião pode, a dada altura, tornar-se ele mesmo a vítima, e a vítima o rufião, pelo que importa conhecer ambos. À vítima importa prestar ajuda no sentido de ultrapassar o assédio e humilhação sentidos, ao rufião importa saber as suas motivações e mudar as suas atitudes.

[Slide 30]

Tal como em muitos outros factos da vida, a prevenção é o melhor meio de evitar os efeitos do cyberbullying. Aqui apresentamos algumas dicas que poderão ser úteis:

- **Conheça as armas de combate ao bullying**

Navegue pela Internet e informe-se acerca de todos os meios de combate à disposição do cibernauta. A vítima não precisa de sofrer passivamente este tipo de ataques, existem formas de resolução, nomeadamente, reportando ao responsável pelo sítio de Internet a situação de abuso ou à operadora de telecomunicações. Se entender que o bullying assume contornos realmente nocivos, contacte a polícia.

- **Fale com o seu filho/educando**

A comunicação entre o jovem e as pessoas envolvidas na sua educação ajuda a evitar o isolamento e o segredo quando um problema destes se instala. Falar regularmente com o seu educando ajuda a perceber as alterações no seu comportamento e a prestar-lhe a ajuda necessária. Em especial, explique ao jovem que ele não está sozinho nesta situação e não tem que passar por ela sozinho, nem fez nada para merecer ser maltratado dessa forma.

- **Mantenha os computadores em locais comuns da sua habitação**

Este cuidado refere-se aos computadores com acesso à Internet. Ao limitar a privacidade na utilização da Internet, poderá estar mais atento a alguma utilização mais abusiva, bem como agir atempadamente caso tal suceda.

- **Não permita a partilha de dados pessoais**

Ensine ao seu educando os perigos de fornecer dados pessoais a terceiros, tais como o roubo de identidade. Além disso, trocar ou colocar imagens pessoais na Internet oferece a oportunidade a outros de as copiar, usar e manipular.

- **Ensine os seus educandos a serem correctos na Internet**

Insista na boa educação, seja online ou no dia-a-dia. Um dos efeitos nefastos do cyberbullying é levar a vítima a retaliar e tornar-se, ela mesma, numa cyberbullying. Quebre este ciclo encorajando o seu educando a responder de forma apropriada (informando os responsáveis pelos sítios de Internet, as operadoras de telemóvel ou ignorando a situação). Não deixe o jovem perder o controlo da sua vida, que é o principal propósito do cyberbully.

Da mesma forma, mostre-lhe que começar neste tipo de “brincadeiras” (que o cyberbully pode considerar inocente, não tendo consciência das consequências para o alvo) é algo muito negativo e perigoso.

- **Guarde as mensagens de cyberbullying**

Embora não sejam agradáveis, estas podem servir de prova caso o assunto assuma proporções tais que seja necessária a intervenção de entidades especializadas.

- **Mude de conta de correio electrónico ou outras**

Se a situação persistir, incentive o jovem a mudar a conta na qual o abuso ocorre, seja correio electrónico, blogue, ou outra. Mantenha as contas antigas para ajudar a apanhar o rufião.

- **Instale software de prevenção de cyberbullying**

Se pesquisar na Internet, encontrará alguns programas que poderá instalar no seu computador para ajudar a prevenir este tipo de situação e/ou ajudar a identificar a origem do ataque.

i. Phishing

[Slide 31]

O “phishing” (trocadilho com “fishing”, ou “ir à pesca” em inglês, dado que a informação é como que um “anzol” que se espera que alguém “morda”) consiste em utilizar métodos vários que levem o cibernauta a revelar dados pessoais e confidenciais, como os seus números de cartão de crédito, informação de contas bancárias, números de segurança social, passwords e outros.

Os “phishers” recorrem a várias formas de obtenção de informação, nomeadamente, SPAM, mensagens de pop-up ou e-mails, fazendo-se passar por empresas ou organizações legítimas com a qual a potencial vítima tem negócios - por exemplo, o seu fornecedor de serviços de Internet (vulgo ISP), banco, serviços de pagamentos online ou até um organismo governamental.

Estas mensagens costumam alegar que o cibernauta precisa de “actualizar” ou “validar” a informação da sua conta, chegando a ameaçar com consequências negativas (o fecho da conta, por exemplo) caso não haja resposta. A estas técnicas de ameaça e manipulação dá-se o nome de Engenharia Social, nas quais também se inserem as formas mais sedutoras de persuasão, como a “oferta” de artigos, viagens ou dinheiro por Internet.

[Slide 32]

A mensagem maliciosa que foi enviada pode reencaminhar a pessoa para um sítio de Internet que parece legítimo, mas na verdade não é. O propósito deste sítio fraudulento é enganá-la no sentido de divulgar informação pessoal que permita aos burlões roubar-lhe a sua identidade e debitar contas ou cometer crimes em seu nome. Outras formas de phishing envolvem subterfúgios técnicos têm como objectivo plantar um programa malicioso no seu computador que irá obter e enviar os dados pretendidos aos seus autores.

[Slide 33]

Pode seguir algumas orientações que poderão ajudar a evitar um logro por este tipo de fraudes:

- **Se receber um e-mail ou pop-up que lhe peça informação pessoal ou financeira, não responda nem clique no link da mensagem.**
- **Lembre-se: empresas legítimas não pedem este tipo de informação por correio electrónico**

Se está preocupado com a sua conta ou se dúvidas quanto ao remetente ou conteúdo da mensagem, entre em contacto com a organização (alegada autora da mensagem) através de um número de telefone que sabe ser legítimo, ou abra uma nova sessão num Internet Browser e aceda ao endereço correcto da empresa.

Em qualquer caso, não copie o link da mensagem.

- **Não envie informações pessoais ou financeiras por e-mail**

O e-mail não é um método seguro para transmissão de informações pessoais. Se iniciou uma transacção através de um sítio de Internet e deseja fornecer dados pessoais ou financeiros através desse sítio, procure indicadores de que o mesmo é seguro, tal como um ícone de um cadeado na barra de status do browser ou um URL que comece com "https:" (o "s" significa "secure"). Infelizmente, nenhum indicador é à prova de falhas; alguns "phishers" já falsificaram ícones de segurança.

- **Veja regularmente os extractos do seu cartão de crédito e contas bancárias para determinar se há débitos indevidos**

De preferência, verifique-os assim que os receber. Se estes extractos se atrasarem mais do que um par de dias, telefone ao seu banco e solicite essa informação.

- **Use software antivírus e mantenha-o actualizado**

Alguns e-mails de phishing contêm software que pode causar danos no seu computador ou monitorizar as suas actividades na Internet sem o seu conhecimento. Um antivírus e uma firewall podem protegê-lo de aceitar inadvertidamente esse tipo de ficheiros.

O software antivírus verifica comunicações recebidas, procurando detectar ficheiros problemáticos. Uma firewall ajuda a torná-lo "invisível" na Internet e bloqueia todas as comunicações de fontes não autorizadas. É particularmente importante ter uma firewall se tem uma ligação de banda larga.

Além de tudo isto, o seu sistema operativo (tal como Windows ou Linux) pode disponibilizar "patches" gratuitos de software para fechar "buracos" de segurança que hackers ou phishers poderiam explorar.

- **Seja cuidadoso no que respeita a abrir qualquer anexo ou descarregar quaisquer ficheiros a partir de e-mails que receba, independentemente do remetente**

Não se esqueça que há vírus que enviam e-mails através de remetentes familiares. O facto de ter o seu computador livre de vírus não implica que os seus amigos e contactos no mundo virtual também estejam na mesma situação.

4. Sítios úteis

[Slide 34]

1. Guia para a segurança na Internet
 - a. <http://www.internetsegura.pt/pt-PT/Biblioteca/manuais/ContentDetail.aspx>
2. Sobre o consórcio Internet Segura
 - a. <http://www.internetsegura.pt/pt-PT/Sobre/ContentDetail.aspx>
3. Sobre Perigos e prevenção
 - a. <http://www.internetsegura.pt/pt-PT/Perigos/ContentDetail.aspx>
4. Portal sobre segurança na Internet para a Comunidade Escolar
 - a. www.seguranet.pt
5. Linha Alerta
 - a. <http://LinhaAlerta.internetsegura.pt>
6. Sítio sobre segurança da Microsoft
 - a. <http://www.microsoft.com/portugal/seguranca/default.msp>