Módulo 2

Conhecer a Rede

Riscos e Desafios

Índice

1 - Navegar na Internet

1.1. Comunicar por e-mail

O que é o e-mail?

O correio electrónico, também conhecido por ***e-mail*** (abreviatura de "electronic mail")**,** permite o envio de uma mensagem para uma ou várias pessoas em qualquer parte do mundo, em poucos segundos.

Também a criação de listas de distribuição, que permitem o envio de um *e-mail* para diversos utilizadores em poucos segundos, é outra das potencialidades oferecidas pelos sistemas de correio electrónico.

Como funciona o correio electrónico?

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

- Possuir uma ligação à Internet;
- Estar registado num servidor de e-mails;
- Escrever a sua mensagem, colocar o endereço electrónico do destinatário no local apropriado;
- Proceder ao seu envio clicando na área apropriada desse mesmo servidor.

Que perigos pode apresentar uma mensagem de correio electrónico?

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 no Módulo 3 - 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 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-mail's em massa. Estes sistemas comprometidos são, com frequência, computadores mal protegidos para utilização "final" (ex.: sistemas domésticos e de pequenas empresas).

Segundo um estudo realizado pela associação norte-americana Pew Internet and American Life Project, 53% dos internautas daquele país passam diariamente cinco minutos ou mais a apagar e-mail's indesejáveis. Um estudo recente, da União Europeia conclui que metade dos e-mail's enviados em todo o mundo eram "spams", mas estimativas avançadas pela Jupiter Research prevêem que esse número suba para cerca de 80 por cento.

Assim, se for confrontado com um e-mail de origem duvidosa, não responda nem clique no *link* "**Remove from mailing list"** (remover da lista de endereços), porque se o fizer está a ajudar a confirmar o seu endereço.

Cuidados a ter

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

- **Correr e manter 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. Utilizar sempre o antivírus para examinar as mensagens e anexos que 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.

- **Ter 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. Esta pasta deve ser verificada com frequência, dado que poderá dar-se o caso de alguma mensagem legítima ser para ali encaminhada por engano.
Deve-se desconfiar das 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 enchem de SPAM.

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

- **Não correr programas de origem desconhecida**

As opções que permitem abrir ou executar automaticamente ficheiros ou programas anexados às mensagens devem ser desligadas.

Não descarregar, instalar ou correr programas a menos que se saiba que este é da autoria de uma pessoa ou companhia em que se confia. Os utilizadores de e-mail devem suspeitar de anexos inesperados. A certificação de que se conhece a origem de um anexo antes de o abrir é fundamental. Não basta que a mensagem tenha origem num endereço que reconhece, dado que os computadores dos 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 enviar 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 se desejar enviar informação confidencial, o melhor é reccorer a e-mails cifrados. Existem várias soluções comerciais ou gratuitas (“freeware”) na Internet que codificam os dados do remetente para o receptor.

- **Usar 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 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.

- **Ter filtros de "gateway" de correio electrónico**

Dependendo das necessidades de cada 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**

1.2. Blogues

O que é um blogue?

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 comunidade 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 (sobre esta última temática falaremos com mais detalhe na secção "Que perigos apresentam?").

Como funcionam os blogues?

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.

Que perigos podem apresentar os blogues?

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 on-line, 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 on-line 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.

Por vezes, este tipo de perseguições virtuais pode passar para o mundo real, pelo que é importante não fornecer qualquer tipo de informação que facilite o contacto pessoal com o bloguista.

- **Imagens**

A colocação de imagens pessoais na Internet pode levar outros a apropriarem-se indevidamente delas. Pensar bem antes de colocar 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 defesa a certas doenças, como a anorexia, que exprimem opiniões que podem levar os mais influenciáveis (nestes casos, crianças e adolescentes) a iniciar e/ou manter comportamentos lesivos para a sua saúde. Outros tipos de blogues perigosos são os de defesa à discriminação, de incitação ao ódio, de defesa do suicídio. Estes devem ser reportados às entidades apropriadas (por exemplo, à Linha Alerta) e afastados dos mais jovens.

- **Responsabilização pelos conteúdos**

O bloguista é responsável pelos conteúdos inseridos no seu blogue. Contudo, esta responsabilização nem sempre é levada a sério, e muitos bloguers 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.

Cuidados a ter

- **Tipo de blogue**

Ao iniciar-se no mundo dos blogues, tenha em atenção a 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 permite, que autores recorrem aos seus serviços e que tipo de respostas existem por parte dos leitores. Se não gostar dos blogues que vir, considere a hipótese de aderir a outro servidor.

- **Não refira o seu apelido, a sua morada ou telefone em lado algum**

Este perigo é tanto mais importante quanto mais jovem for o bloguista. Há predadores on-line que procuram nos conteúdos dos blogues as fraquezas das suas potenciais vítimas, bem como dados que os levem a elas pessoalmente. No caso de bloguistas maiores de idade, também é importante ter em atenção que há indivíduos que podem ficar inflamados com as opiniões apresentadas e procurar resolver esse "insulto" ao vivo. 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. Por exemplo, se referir que é estudante e colocar um link da sua escola, será fácil a alguém mal 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 tipos de imagens pessoais na Internet, para evitar a perseguição por parte de predadores on-line.
Se, ainda assim, o utilizador desejar colocar imagens pessoais no seu blogue e estas focarem terceiros, deverá pedir a autorização deles 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. Envolva-se nas actividades on-line dele e ajude-o a tomar decisões conscientes e educadas, de modo a não se colocar em risco ou provocar desentendimentos com terceiros.

1.3. Chamadas telefónicas através da Internet – VoIP

As inovações tecnológicas vieram facilitar a possibilidade de apreciar as vantagens da realização de chamadas telefónicas através da Internet, também conhecidas como "Voz sobre IP" (ou VoIP - *Voice over Internet Protocol*).

Contudo, à medida que o serviço se torna mais comum, os criminosos e burlões on-line viraram as suas atenções para esta nova ferramenta. Antes de se experimentar um serviço de VoIP, é aconselhável obter informação sobre as vantagens e desvantagens deste sistema, e conhecer os passos que se devem tomar para melhorar a segurança.

Vantagens dos sistemas de Voz sobre IP

O serviço de Voz sobre IP para consumidores finais está a expandir-se rapidamente em todo o mundo, oferecendo alguns aspectos positivos tanto para utilizadores de telefones fixos, como para utilizadores de telemóveis:

- Fácil instalação e utilização.

Em muitas áreas, não é necessário de um computador para começar; o serviço está disponível através do telefone, usando um pequeno adaptador.

- Armazenamento de telefonemas.

Pode se aceder on-line ao correio de voz do sistema de Voz sobre IP, guardar conversas telefónicas no computador e reproduzi-las quando se quiser.

Riscos dos sistemas de Voz sobre IP

- Roubo.

Os intrusos que conseguirem aceder a um servidor VoIP podem ter acesso aos dados de voz arquivados e ao próprio serviço, usando-o para realizarem escutas ilegais ou usarem a conta para fazerem chamadas gratuitas.

- Ataque por vírus.

Se o computador de um servidor VoIP for infectado por um vírus, isso pode resultar na perda total do serviço telefónico dos clientes. Pode também afectar outros computadores ligados ao sistema.

- Tecnologia não-regulamentada.

Apesar de estarem a ser desenvolvidas algumas iniciativas de regulamentação, actualmente os utilizadores estão sujeitos a algumas vulnerabilidades e esquemas fraudulentos específicos. Por exemplo, as empresas de *telemarketing* podem usar o VoIP para distribuir quantidades astronómicas de mensagens de voz automáticas para os consumidores, o que pode provocar que o sistema vá abaixo. Os criminosos podem também usar um processo a que se dá o nome de *caller ID spoofing* (ocultação ou camuflagem da identidade de quem faz uma chamada) para cometer fraudes. Podem fazê-lo anunciando-se como uma entidade oficial e tentando levar à divulgação de informações sensíveis relacionadas com contas.

Para aumentar a segurança na utilização de sistema de Voz sobre IP

- **Manter palavras-passe seguras e robustas.**

Criar palavras-passe seguras para aceder aos sítios Web de serviços que armazenam o correio de voz e outros dados de áudio. Não os divulguar a ninguém.

- **Manter o computador pessoal seguro.**

Se usa um computador para aceder ao correio de voz e conta VoIP a partir do sítio Web de um fornecedor de serviços, deve ajudar a manter a segurança do sistema protegendo o computador com palavras-passe seguras, com uma *firewall*, com software anti-vírus e com software actualizado.

1.4. YouTube

O que é o YouTube?

É um serviço gratuito de emissão de vídeos que permite a qualquer utilizador ver e partilhar vídeos enviados por membros registados.

Existem algumas regras elementares de utilização que o próprio site refere e que são aqui descritas de uma forma simplificada:

- O YouTube não serve para divulgar conteúdos de pornografia ou sexo explícito.
- Não deverão ser publicados vídeos mostrando situações nefastas como o maltrato de animais, o abuso de drogas, ou equivalente.
- Violência gratuita não é permitida, bem como situações que reportem apenas imagens chocantes.
- Os direitos de autor deverão ser respeitados.
- É encorajada a liberdade de expressão, mas não é permitido discursos extremistas sobre: sexo, orientação sexual, raça, religião, origem étnica, idosos, cor, idade, deficiência ou nacionalidade.
- Há tolerância zero para o comportamento predatório, stalking, ameaças, assédio, invasão de privacidade, ou o revelar informações pessoais de outros utilizadores.
- Não divulgar spam. Não criar descrições enganosas, marcas, títulos ou miniaturas.

Mais informação sobre as regras de segurança a adoptar na utilização do YouTube em: http://www.youtube.com/t/safety.

2 - Comunidades Virtuais

2.1. O que é uma rede social virtual ou uma comunidade virtual?

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.

Como funcionam as redes sociais virtuais?

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. Quanto mais amigos figurarem nessa lista, mais popular será considerado o utilizador, um factor tanto mais importante quanto mais jovem for. 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.

Que perigos podem apresentar as redes sociais virtuais?

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 on-line, que procuram activamente formas de contactar pessoalmente as suas potenciais vítimas.

Este perigo não se aplica somente aos mais novos: por exemplo, referir os rendimentos anuais é convidar sujeitos mal-intencionados a tentar a exploração. Se, além dos rendimentos, for referido também a 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 on-line e na vida real.

Por outro lado, é frequente alguns empregadores pesquisarem as informações colocadas on-line 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 on-line. 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.

Cuidados a ter

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 dados pessoais**

Nunca coloque informação que possa levar alguém a encontrá-lo(a). Dados sobre o local onde reside, trabalha, números de telefone, devem ser completamente omitidos. 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.

As regras acima apresentadas servem para todos aqueles que pretenderem ter uma utilização o mais segura possível das redes sociais virtuais. Contudo, dado que estas são bastante populares junto dos mais novos, aqui ficam também algumas regras que os educadores devem fazer cumprir junto dos seus educandos:

- **Colocar os perfis como privados**

Alguns sítios Web optam por considerar privados os perfis dos utilizadores de uma determinada faixa etária, bloqueando-os do acesso geral. Os dados das páginas privadas apenas são visíveis pelas pessoas na lista de amigos desse utilizador, o que lhe proporciona uma segurança adicional. Caso o sítio onde o jovem está inscrito não possua esta funcionalidade automatizada, é aconselhável ele mesmo torne a sua página privada.

- **Aceitar apenas utilizadores que conhece pessoalmente**

Se apenas aceitar ter na sua rede de amigos aqueles que já conhece pessoalmente, o jovem diminui muito as probabilidades de ser abordado por um predador on-line, ou até de ser vítima de cyberbullying.

- **Não aceitar conhecer os amigos virtuais pessoalmente**

Nem toda a gente é na realidade o que diz ser na Internet. Há relatos de crianças raptadas, abusadas e violadas por predadores on-line que conseguiram acesso a elas pessoalmente.

Se, porventura, o educador aceder que o seu educando conheça um amigo virtual pessoalmente, deve ir com ele ao encontro, que deverá ser num local público, frequentado por muitas pessoas (por exemplo, um centro comercial) e de dia. Caso o seu educando insista em encontrar-se com alguém sem a sua presença, não o autorize e explique o porquê de tal atitude.

- **Cuidado com as fotografias**

Fotografias reveladoras do local onde foram tiradas podem tornar um jovem vulnerável a encontros pessoais por parte de predadores on-line.

Outra forma de vulnerabilidade prende-se com a colocação de fotografias de natureza provocante. Há jovens que procuram aceitação social através da exposição do seu corpo. Explique ao seu educando quais os perigos de o fazer. Ser alvo do desejo de indivíduos mal-intencionados pode conduzir o menor a perigos desnecessários on-line e/ou na vida real.

- **Não colocar informações sobre terceiros**

O jovem deve estar atento para não colocar dados na sua página pessoal que revelem informações sobre os amigos. Estas informações, se puderem levar à sua identificação, podem colocá-los em perigo desnecessário. Fale com o seu educando acerca destes perigos e da necessidade de pedir sempre autorização sempre que quiser colocar qualquer tipo de informação que refira um(a) amigo(a).

2.2. Conviver na Internet

Navegar na Internet pode ser algo divertido, útil e social. No entanto, é importante que todos os novos cidadãos da Internet, também chamados *netcitizens*, se lembrem de que existem igualmente outros cidadãos. E, tal como na navegação real ou noutra actividade pública, existem regras implícitas de conduta, ou convivência. Sugerimos algumas regras básicas de convivência na Internet:

Ter sempre uma boa conduta

Se não compreendermos como funcionam as regras de cidadania na Internet, isso poderá resultar em muito mais do que a simples perda de uma boa oportunidade. Se se disser algo errado, na altura errada, isso poderá ser considerado um abuso e provocar outros problemas. Aqui ficam algumas orientações:

- Tratar os outros como gostaria de ser tratado.
- Lembrar de que existe uma pessoa no outro lado da mensagem.
- Adoptar um comportamento adequado ao espaço em que se está.
- Perdoar os erros das outras pessoas, especialmente os principiantes.
- Permanecer sempre calmo, especialmente se alguém o insultar.
- Evitar as MAIÚSCULAS, pois alguns utilizadores entendem isto como

"gritar."
- Não utilizar linguagem inadequada ou ofensiva.
- Utilizar o nome ou alcunha on-line de forma consistente e assinar todas as mensagens da mesma forma (protegendo, no entanto, a identidade).
- Não enviar ou reencaminhar correio electrónico publicitário.
- Não se envolver em discussões prolongadas e pessoais.
- Verificar a ortografia das mensagens e manter as mensagens curtas.
- Quando se está em salas de chat, não interromper os outros e falar apenas do tópico em discussão.
- Seguir as mesmas regras de bom comportamento que se teria na vida real.

Utilizar símbolos expressivos

Dado que muitas vezes é difícil transmitir emoções, intenções, ou tom, apenas com o texto, os primeiros utilizadores da Internet inventaram símbolos expressivos, ou *emoticons*, que são expressões faciais virtuais criadas a partir de caracteres do teclado, tal como a vírgula e o parêntesis curvos. Aqui se encontram alguns exemplos dos símbolos mais utilizados:

- :-) Feliz ou a brincar
- ;-) A piscar o olho
- :-(Triste
- :-| Ambivalente
- :-o Surpreendido, ou preocupado
- :-x Sem dizer nada
- :-p Com a língua de fora (normalmente a brincar)

As siglas mais usadas on-line

Outra ideia que evoluiu para facilitar as comunicações é a utilização de siglas. Uma vez que se pode falar mais rápido do que se escreve, pode reduzir as frases mais comuns para algumas letras simples. Se se encontrar uma sigla que nunca se viu, o melhor é perguntar com educação o que significa e passarás a ter um excelente vocabulário de siglas! Aqui estão alguns exemplos das siglas mais utilizadas:

- ASAP (As Soon As Possible - O mais depressa possível)
- BBL (Be Back Later - Volto mais tarde)
- BRB (Be Right Back - Volto já)
- LOL (Laughing Out Loud - Gargalhada)
- BTW (By The Way - A propósito)
- OIC (Oh, I See - Agora percebo)
- CUL (See You Later - Até logo)
- RUOK (Are You OK? - Estás bem?)
- TIA (Thanks In Advance - Agradeço desde já)

- J/K (Just Kidding - Estava a brincar)
- TTFN (Ta-Ta For Now - Até já)

2.3 Plataformas CMS e LMS

CMS
As plataformas gestoras de conteúdos (*Content Management Systems* – CMS), são sistemas que permitem gerir websites, portais e intranets. As CMS integram ferramentas que possibilitam criar, editar e inserir conteúdo, sem a necessidade de possuir conhecimentos de programação, facilitando a distribuição, publicação e disponibilidade da informação.

LMS
As plataformas gestoras de aprendizagem (*Learning Management Systems* – LMS) são softwares desenvolvidos sobre uma metodologia pedagógica para auxiliar a promoção do ensino/aprendizagem à distância ou semi-presencial. Estas plataformas contêm um vasto número de ferramentas, como por exemplo os e-mails, fóruns, conferências, chats, arquivos de textos, wikis, blogs, etc. Destaca-se que nestes ambientes, textos, imagens e vídeos podem circular de maneira a potencializar o poder da educação através da comunicação. Permitem ainda a possibilidade de criar hiperligações fomentando o aumento do conhecimento.
A LMS mais utilizada a nível nacional é o *Moodle* (*Modular Object-Oriented Dynamic Learning*) criado em 2001 por Martin Dougiamas. Esta plataforma é um software opensource, que pode ser instalado em diversos sistemas operativos. É desenvolvido por uma comunidade virtual que reúne programadores e investigadores de software opensource, administradores de sistema, professores e utilizadores de todo o mundo. No bloco de administração existe uma componente de segurança.

Tanto as CMS, como as LMS são sistemas que permitem a criação de contas de utilizador, servindo-se para o efeito de um endereço de E-mail para a confirmação do seu registo. Desta forma, para evitar o roubo de identidade são necessárias utilizar algumas regras básicas: Criar uma palavra-chave segura, não a divulgar a terceiros e no final da sessão não esquecer do botão saída (encerrar a sessão).

2.4 Hi5 e MySpace

O Hi5 é um fenómeno de sucesso à escala mundial, que funciona como uma base de dados de pessoas a nível internacional. Para fazer parte desta base de dados é necessário efectuar um registo pessoal, fornecendo um endereço de e-mail. Depois, cada utilizador pode preencher um formulário sobre si, que disponibiliza o seu perfil para os outros utilizadores, juntamente com fotografias. O processo é rápido e simples.

Sugestões de segurança para a utilização desta comunidade virtual, dirigida aos adolescentes e aos encarregados de educação, pelo próprio hi5.

Sugestões de Segurança On-line para Adolescentes

O hi5 pode ser um local divertido para estar em contacto com amigos, criar conteúdos e trocar ideias, mas é importante lembrar que, ao utilizar o hi5 ou a Internet em geral, as informações publicadas podem causar embaraços ou expor o utilizador a situações perigosas. São, em seguida, apresentadas algumas directrizes de bom senso que deverás seguir ao utilizar o hi5 ou a Internet:

- **Protege as tuas informações**. Utiliza as definições de segurança para controlar quem pode visitar o teu perfil. Lembra-te de que se não utilizares as funções de segurança, qualquer pessoa pode aceder às tuas informações. Evita publicar informações que te tornem fácil de localizar por estranhos.
- **Nunca te encontres com estranhos**. Evita encontros com alguém que conheças on-line. Se tiveres de te encontrar com um amigo on-line, marca o encontro num local público, durante o dia e pede a um parente próximo para te acompanhar.
- **Fotografias: Pensa antes de publicares algo**. Evita publicar fotografias que permitam a tua identificação (por exemplo, se alguém efectuar uma pesquisa pela escola que frequentas) ou que contenham imagens especialmente sugestivas. Antes de transferires uma fotografia, pensa em como te sentirias se esta fosse vista por um pai/avô, professor de universidade ou futuro empregador.
- **Verifica os comentários regularmente**. Se permitires comentários ao teu perfil, verifica-os regularmente. Não respondas a comentários ou emails maldosos ou embaraçosos. Elimina-os, não permitas comentários de pessoas ofensivas e comunica a identidade das mesmas ao hi5. Além disso, nunca respondas a emails de estranhos que façam perguntas pessoais.
- **Sê honesto em relação à tua idade.** As nossas regras de filiação existem para proteger os utilizadores. Se mentires acerca da idade, o hi5 eliminará o teu perfil.
- **Confia nos teus instintos se suspeitares de algo.** Se te sentires ameaçado por alguém ou desconfortável por algo on-line, conta a um adulto em quem confies e informa a polícia e o hi5.
- **Informações adicionais.** Para obter informações adicionais sobre segurança on-line e para saber mais, consulte também estes recursos: http://www.blogsafety.com e http://onguardonline.gov/socialnetworking_youth.html

Sugestões de Segurança On-line para os Pais

A Internet pode ser um local divertido e útil para os adolescentes. Mas, do mesmo modo que outros locais públicos, encontra-se igualmente cheia de riscos e potenciais perigos. Ninguém pode garantir total segurança on-line aos adolescentes. Contudo, os pais e os tutores desempenham o papel mais importante nesta função. Os pais devem empregar todos os esforços no

sentido de falar abertamente com os adolescentes sobre as experiências on-line e procurar apoio e aconselhamento junto de outros pais, educadores, especialistas de segurança on-line e dos próprios adolescentes. Cada pai deverá desenvolver um plano de segurança on-line para os seus filhos adolescentes. Seguem-se algumas sugestões e directrizes:

- **Seja sincero com os seus filhos** e encoraje-os a falar consigo se tiverem problemas on-line— desenvolva a confiança e a comunicação, uma vez que não há regras, leis ou software de filtragem que o substituam como a primeira linha de defesa de um adolescente.
- **Fale com os seus filhos** sobre a forma como utilizam os serviços. Certifique-se de que entendem as directrizes de segurança básicas da Internet e de redes sociais. Estas incluem proteger a privacidade (incluindo a utilização de palavras-passe), nunca publicar informações de identificação pessoal (como, por exemplo, o apelido, número da Segurança Social, número de telefone da residência ou números de cartão de crédito), evitar encontros pessoais com pessoas que conheçam on-line e não publicar fotografias impróprias ou potencialmente embaraçosas. Sugira que utilizem as ferramentas de privacidade do hi5 para partilhar informações apenas com pessoas que conhecem realmente (e não apenas virtualmente) e nunca admitir "amigos" nas suas páginas, excepto se souberem quem são.
- **Considere estabelecer que todas as actividades on-line tenham lugar numa área central da casa**, não no quarto dos seus filhos. Tenha em atenção que poderão existir outras formas de as crianças poderem aceder à Internet fora de casa, incluindo em vários telemóveis e consolas de jogos.
- **Tente que os seus filhos partilhem blogs ou perfis on-line** consigo. Utilize motores e ferramentas de pesquisa em páginas de redes sociais para procurar o nome completo do seu filho, o número de telefone e outras informações identificadoras.
- **Diga aos seus filhos para confiarem nos seus instintos no caso de suspeitarem de algo.** Se se sentirem ameaçados por alguém ou desconfortáveis por algo on-line, devem contar-lhe e, em seguida, informar a polícia e o hi5.
- **Informações adicionais.** Para obter informações adicionais sobre segurança on-line e para saber mais, consulte também estes recursos: http://www.blogsafety.com e http://onguardonline.gov/socialnetworking.html

Para mais informações consultar: http://www.hi5.com/friend/displaySafety.do

My Space é outra comunidade virtual, com o objectivo de permitir aos utilizadores expressar-se, publicando seus pensamentos, fotografias e interesses. Neste espaço são fornecidas algumas sugestões de segurança, tais como, vídeos explicativos, dicas de segurança dirigidas a encarregados de educação e adolescentes, recursos de segurança e dicas gerais de segurança. Mais informações em http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagehome.

2.5 Fórum

Fórum é uma aplicação destinada a promover debates através de mensagens publicadas. Existem fóruns sobre os mais diversos temas ou assuntos. Estes podem estar incluídos em páginas Web temáticas, onde o administrador permite que os visitantes possam colocar questões ou dar sugestões, ou podem ser apenas páginas Web dedicadas ao próprio fórum.

O membro com estatuto de administrador é o que agrega as funções de administração e configuração do fórum, criação de adequação de novas salas, é quem tem permissão para enviar e-mails em massa, é quem pode bloquear, suspender ou expulsar outros membros, entre inúmeras outras funções administrativas. Muitas vezes, também se pode encontrar moderadores com algumas funções de administradores (como bloquear utilizadores), ou administradores com menos permissões que outros.

2.6 Chats e IM

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.

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, consequentemente, podem apresentar alguns perigos, sobretudo para os cibernautas mais jovens (por exemplo, um menor pode, inadvertidamente, conversar com um pedófilo).

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 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 on-line.

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).

O *MSN Messenger* é uma das ferramentas da Internet mais utilizadas actualmente por jovens e adultos. A comunicação é uma das principais actividades da Internet, no entanto são bem conhecidos os seus riscos. Neste sistema, ao contrário das chatrooms, cada utilizador define a sua lista de contactos e tem o poder de aceitar ou recusar a adição de pessoas à sua lista.

Que perigos podem apresentar os chats e os IMs?

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 se deve estar atento é o *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 (veja Módulo 3 - *Phishing*).

Cuidados a ter

Seguidamente, apresentamos 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.

- **Escolha um nome de utilizador (username) que não revele informação pessoal**

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.

- **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 (veja cyberbullying).

- **Não divulgue informação privada a desconhecidos**

Tenha sempre em mente que, por mais que julgue conhecer uma pessoa com quem falou on-line, 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.

- **Não aceite encontrar-se com desconhecidos**

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.

- **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 on-line. Este tipo de registo já se provou útil para o decurso de investigações a predadores na Internet.

Alguns conselhos de segurança para os mais novos relativamente à utilização das salas de chat:

Conselhos de segurança para as salas de chat:

1. Nunca dês os teus dados pessoais numa sala de chat.
2. Nunca aceites encontrar-te pessoalmente com alguém que tenhas conhecido numa sala de chat.
3. Quando te pedirem para introduzires ou registares uma alcunha para o chat, selecciona um nome que não revele dados pessoais. Por exemplo, usa SolMar em vez de SaraOeiras.
4. Desconfia das pessoas que te convidam para passar para salas de chat privadas.
5. Antes de participares, verifica os termos e condições, o código de conduta e a declaração de privacidade no sítio onde se encontra alojado o chat.

Alguns conselhos de segurança para os mais novos relativamente à utilização das IM:

Conselhos de segurança para as IM:

- Escolhe uma alcunha que não coloque em evidência os teus dados pessoais.
- Na edição do perfil ou em áreas públicas não colocar dados pessoais de modo a evitar mensagens instantâneas indesejadas.
- Nunca fornecer dados pessoais (nº de cartão de crédito, palavras chave, etc) numa conversa de IM.
- Tenta comunicar apenas com pessoas que se encontram na tua lista de contactos.
- Não aceder encontrarmo-nos pessoalmente com alguém que apenas conhecemos por IMs.
- Nunca transferir imagens, ficheiros ou em hiperligações de IMs de pessoas que desconhecemos.

2.7. Riscos: Cyberbulling e Predadores On-Line

O que é o Cyberbullying?

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.

Como funciona o cyberbullying?

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 prazer advindo 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-chave 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-chave 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 on-line, 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 sub-repticiamente 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-chave (veja "Roubo de identidade ou de palavras-chave", 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 (veja phishing).

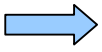
Que perigos pode apresentar o cyberbullying?

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 de tal forma graves que levem a vítima a cometer suicídio.

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.

Aos educadores cabe um papel importante na prevenção do bullying.



Cuidados a ter

Tal como em muitos outros factos da vida, a prevenção é o melhor meio de evitar os efeitos do cyberbullying. 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, à operadora de telecomunicações ou encaminhando o assunto para uma hotline, tal como a Linha Alerta. 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 (veja “Como funciona?”). 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 on-line 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, os servidores de telemóvel, usando uma hotline como a Linha Alerta 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 forças 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.

Predadores On-Line

Haverá alguma forma melhor de conhecer pessoas do que através da Internet? Graças às salas de conversação da Internet, fazem-se grandes amizades. Algumas pessoas casam-se, outras encontram parceiros de negócios. A Internet é aquilo a que os economistas chamam "um mercado eficiente": a partir do nosso computador podemos facilmente encontrar pessoas que partilham os nossos gostos, os nossos pontos de vista, os nossos desejos. É um meio acessível que junta pessoas de todo o mundo, a qualquer hora.

Actualmente é usual ter amigos que não se conhece pessoalmente. Os dois maiores sites de redes sociais da Internet têm mais de 100 milhões de membros em todo o mundo, que conversam, partilham notícias e boatos e trocam fotografias.

No entanto existe um lado negativo

A Internet tornou-se uma óptima forma de conhecer novas pessoas que partilham interesses, no entanto nem sempre se tem a certeza quem é a pessoa com quem se está a comunicar no ciberespaço. Recentemente, mais de 40 raparigas adolescentes do Reino Unido foram contactadas por um pedófilo do Canadá, que obteve os seus endereços electrónicos entrando numa "lista de amigos" de uma adolescente – uma lista das suas amigas da Internet. Felizmente, foi apanhado e levado a tribunal. Mas trata-se de um problema crescente. Nos Estados Unidos, o FBI calcula que existam mais de 50 000 pedófilos que actuam na Internet, em todo o mundo, em qualquer momento, e um em cada 12 adolescentes já se encontrou pessoalmente com um estranho com quem tinha conversado na Internet.

Os pedófilos costumam procurar potenciais vítimas nas salas de conversação. Depois de estabelecido um primeiro contacto, a vítima é "preparada" para um encontro face a face através de uma série de conversas que procuram criar uma relação de confiança. Este fenómeno é conhecido por "grooming" e a polícia por vezes vigia as salas de conversação à procura de criminosos.

Mas as salas de conversação podem ser utilizadas com objectivos ainda mais sinistros e perigosos. As chamadas "salas suicidas" fornecem informações práticas a pessoas que se querem suicidar. Houve jovens que se suicidaram depois de visitarem uma destas salas, por vezes após a celebração de pactos suicidas com amigos virtuais.

As pessoas gostariam que estes sites fossem ilegalizados e encerrados, mas o policiamento da Internet é particularmente difícil.

Quem se encontra em risco?

Os jovens mais vulneráveis aos "predadores" on-line tendem a ser:

- Novos na actividade on-line e desconhecedores das normas de conduta na Internet;
- Utilizadores intensivos de computadores;
- Utilizadores que gostam de experimentar actividades novas e excitantes na vida;
- Pessoas que procuram activamente atenção ou afecto;
- Rebeldes;
- Isolados ou solitários;
- Curiosos;
- Pessoas confusas no que respeita à identidade sexual;
- Facilmente enganados pelos adultos;
- Atraídos por sub-culturas, à margem do mundo dos seus pais;

Alguns conselhos de segurança para os mais novos:

Conselhos de Segurança:

- Verifica os termos e condições, o código de conduta e a política de privacidade do site antes de começares a conversar. Ficarás a conhecer alguns conselhos de segurança valiosos sobre o que deves e não deves fazer.
- Não reveles qualquer informação pessoal (morada, nome da escola, número de telefone) porque podes vir a ser contactado por pessoas que não conheces nem queres vir a conhecer.
- Escolhe uma alcunha que não revele qualquer informação pessoal. Por exemplo, podes usar uma alcunha do tipo JoãoFeliz.
- Nunca transferir imagens a partir de uma origem desconhecida podem ser sexualmente explícitas.
- Utilizar filtros de correio electrónico.
- Falar imediatamente com um adulto caso alguma coisa que aconteça on-line te faça sentir pouco à vontade ou assustado.
- Escolher um nome de ecrã não indicador de sexo, que não contenha palavras sexualmente sugestivas ou revele informações pessoais.
- Interromper qualquer comunicação por correio electrónico, conversa através de mensagens instantâneas, ou chats, se alguém começar a fazer perguntas demasiado pessoais ou com sugestões sexuais.
- Se decidires conhecer pessoalmente o teu amigo da sala de conversação:

- Tenta confirmar antecipadamente se a pessoa é de facto quem afirma ser;
- NUNCA combines encontrar-te com essa pessoa sozinho:

- Se tens mais de 18 anos, faz-te acompanhar por um grande grupo de amigos;
- Se tens menos de 18 anos, deves ir acompanhado de um dos teus pais;
- Se não te sentes à vontade com a ideia de os teus pais ou amigos; conhecerem essa pessoa, não te deves encontrar com ela!
- Combina o encontro num local público e afasta-te de locais isolados (espaços verdes, parques de estacionamento, saídas de emergência...)

3 - Ciberdependência

3.1 Apostas

Os jogos de azar estão a espalhar-se pela Internet a um ritmo alucinante. Em vez de se sair para fazer uma aposta ou ir a um casino, basta aceder à Internet. Mas este tipo de jogo é particularmente viciante porque, ao contrário dos jogos tradicionais, os sites de jogo da Internet nunca fecham e passando horas on-line, deixa-se de ter a noção de que se está a perder dinheiro real.

No Reino Unido, um jovem de 23 anos admitiu roubar mais de 1,5 milhões de euros à sua entidade patronal para financiar o seu vício do jogo on-line. Na pior fase do seu vício, estava a desviar cerca de 25 000 euros diariamente da empresa para as suas contas de jogo.

Muitos adolescentes exploram a Web em busca de actividades excitantes, e por vezes, à procura de um site com um jogo novo, podem descobrir jogos associados a apostas, alguns envolvendo dinheiro real. A maior parte dos jogos e outras actividades on-line são legais e podem ser usadas por menores, mas isso não acontece com as apostas on-line.

Qual é a diferença entre jogos on-line, sites de apostas e sites de apostas a dinheiro?

- **Os sites de jogos on-line** normalmente incluem jogos do tipo dos jogos de tabuleiro, jogos de cartas, questionários, puzzles, ou jogos electrónicos (do tipo dos existentes nos salões de jogos), nos quais os jogadores batem recordes de pontuação. Não há nenhumas transferências de dinheiro, seja ele real ou artificial.

- **Os sites de apostas** podem incluir diferentes tipos de jogos nos quais os jogadores ganham ou perdem dinheiro artificial.

- **Os sites de apostas a dinheiro** normalmente implicam perder ou ganhar dinheiro a sério.

3.2 Jogos On-line

Uma das actividades preferidas dos jovens é jogar, quer seja em consolas ou on-line. Alguns jogos on-line de personagens de fantasia envolvem milhares de jogadores de todo o mundo. Cada jogador é representado por um avatar – uma pessoa imaginária. O avatar pode passar a diferentes níveis lutando contra inimigos e fazendo conquistas, ganhando novas armas, armaduras e habilidades no caminho. Há um jogo que tem mais de quatro milhões de jogadores em todo o mundo e, em qualquer altura do dia, há cerca de 500 000 jogadores on-line.

Em média, um jogo dura cinco ou seis horas e alguns jogadores sentem que a sua vida gira à volta deste mundo cibernético de fantasia. Não há nada de errado em navegar na Internet, desde que os utilizadores tenham uma vida própria para lá do mundo de fantasia do ecrã do computador.

Alguns conselhos a transmitir aos mais novos no sentido de aproveitarem ao máximo esta forma de entretenimento, conhecendo os cuidados para evitar situações de perigo:

1. Informa-te sobre as classificações dos jogos e as declarações de privacidade, e vê os termos de utilização aceitável de todos os sítios de jogos on-line.

2. Tenta jogar sempre com amigos *off-line*, evitando conversar com desconhecidos.

3. Nunca reveles informações pessoais (por exemplo, o nome, a idade, o sexo, ou o endereço de casa), nem mostres fotografias tuas ou de amigos e familiares.

4. Nunca aceites encontrares-te com alguém pessoalmente quando utilizares salas de chat e se alguém te fizer essa proposta, avisa os teus pais.

5. Escolhe nomes de ecrã ou de personagens adequados. Não te esqueças que estes nomes devem respeitar as regras do sítio de jogos, não devem ser reveladores de nenhuma informação pessoal, nem ser um convite potencial a assédio.

6. Se um jogador utilizar linguagem inadequada, antes de mais, conversa com aos teus pais sobre o que aconteceu. Depois podes tentar seleccionar o nome da pessoa em questão na lista de jogadores e s bloquear as suas mensagens, ou denunciá-lo aos administradores do jogo, através de correio electrónico, chat, ou secções de feedback.

7. Utiliza a conversação por voz (*voice chat*) de forma sensata. Lembra-te sempre que a tecnologia de disfarce de voz, que já se encontra disponível para computadores e para a maioria das consolas de jogos, pode ser utilizada por alguns adultos com intenções enganosas.

8. Fica atento a situações de assédio e intimidação em jogos on-line (também conhecidos como *griefers* ou *cyberbullies*). Se sentires que isso te está a acontecer, conversa de imediato com os teus pais.

9. Sempre que te sentires pouco à vontade com alguma coisa que se esteja a passar num jogo, deves parar de jogar e informar os teus pais sobre esse facto, para que estes possam registar e comunicar o problema, se tal for necessário.

10. Convida os teus pais para jogarem contigo on-line. Assim, poderão compreender melhor o teu interesse por estas tecnologias e ajudar-te, no caso de surgir algum problema.

Lidar com a intimidação on-line

A maior parte das pessoas aprecia os jogos on-line e utiliza-os de forma saudável. No entanto, existem cada vez mais jogadores que gostam de assediar e intimidar os outros. Estes jogadores são conhecidos por *griefers*.

Como reconhecer um *griefer*

- Censuram os outros, especialmente os novatos (também conhecidos como *newbies*);
- Atrapalham os companheiros de equipa durante o jogo
- Utilizam linguagem inadequada
- Fazem batota
- Formam grupos itinerantes com outros *griefers*
- Bloqueiam entradas
- Utilizam o jogo simplesmente para aborrecer um alvo conveniente ou para incomodar um determinado jogador que tenha reagido às suas maldades.

Apesar de constituírem apenas uma pequena percentagem da comunidade de videojogos, muitos sítios e fornecedores de jogos estão menos tolerantes para com os *griefers* e recorrem a novos métodos para vigiar a sua presença, tentando limitar o seu impacto.

Mesmo assim, é importante saber lidar com estas situações no caso de acontecerem. Algumas sugestões para os mais novos:

Sugestões para lidar com os *griefers*:

1. Ignora a acção dos *griefers*. Se não reagires às provocações, na maior parte dos casos eles aborrecem-se e deixam de te incomodar.
2. Altera as opções do jogo. Joga com regras ou opções alteráveis, que impeçam determinadas tácticas, como a eliminação de companheiros de equipa.
3. Cria um jogo privado. A maior parte dos mais recentes videojogos para vários jogadores e sítios relacionados permitem que os jogadores formem os seus jogos exclusivos, em que apenas os amigos estão autorizados a jogar.
4. Joga em sítios com regras rigorosas. Escolhe sítios de jogos com códigos de conduta, termos de serviço de cumprimento obrigatório, que tenham administradores de jogo em directo e que possam banir os

griefers.

5. Faz outra coisa qualquer. Se um *griefer* continuar a incomodar-te, experimenta um outro jogo ou faz um intervalo e volta mais tarde ao jogo.
6. Comunica falhas no jogo. Se descobrires falhas dos jogos ou métodos de fazer batota, comunica-as ao administrador do sítio de jogos.
7. Joga jogos que limitem as formas de intimidação. Procura jogos mais recentes, que ofereçam recursos específicos para lidar com os *griefers*, tais como comunicar aos administradores de jogos a presença de formas de intimidação e bloquear ou silenciar mensagens.
8. Não combatas o fogo com fogo. Não utilizes tácticas de intimidação contra um *griefer*, pois o mais provável é que tal atitude conduza a mais comportamentos incorrectos ou, ainda pior, tu próprio poderás ser rotulado como *griefer*.
9. Evita nomes provocadores. Podes prevenir alguns problemas se evitares nomes de ecrã ou alcunhas (muitas vezes referidos como *gamertags*) que possam encorajar maus comportamentos.
10. Não reveles informações pessoais. Os *griefers* (ou outras pessoas) podem usar essas informações (nomes verdadeiros, números de telefone e endereços postais ou de correio electrónico) para te incomodar ainda mais ou para causar outros problemas.

3.3 Riscos: Ciberpatologia

Na Europa e nos Estados Unidos, existem vários estudos que comprovam que o uso exagerado e intensivo da Internet pode trazer problemas de subordinação. Vários psiquiatras falam mesmo de casos de patologia e lançam o alerta.

Não são apenas o álcool, a droga ou o jogo a serem acusados de provocar dependência. Também a Internet pode "viciar" os utilizadores. De facto, um estudo norte-americano de 2006 evidenciava que um em cada três utilizadores passa entre cinco a seis horas diárias ligado à Internet e são conhecidos casos de casais que se divorciaram pelo facto de um dos cônjuges se ter tornado dependente da Internet. Nos Estados Unidos, o número de ciberdependentes ronda os dez por cento dos utilizadores.

Na Europa, nomeadamente na Alemanha, onde já existe uma clínica especializada em tratamento da ciberdependência, um estudo realizado revela existirem cerca de 800 mil utilizadores que navegam, em média, 34 horas por semana. Com efeito, quem passe mais de 24 horas por semana ligado à Internet é considerado como tendo problemas de adição, uma doença por muitos considerados "a doença das novas tecnologias".

Ainda, segundo um estudo realizado em Espanha, concluiu-se que 30% dos utilizadores estão em risco de se tornar dependentes, enquanto cerca de 1 em cada dez revela já sintomas que denunciam um uso problemático dos serviços da Internet. Os responsáveis pelo estudo consideram os resultados

inquietantes e são unânimes em afirmar que, em muitos casos, a dependência se deve a um efeito de substituição, isto é, a maioria das pessoas "em risco" revelou ter dependências anteriores, (álcool, drogas, apostas, etc.).

Assim, o que motiva algumas pessoas a ligarem-se à Internet é a possibilidade de satisfazerem, de forma privada e mais ou menos oculta, as necessidades resultantes de outro tipo de dependências. Daí, que os números apontados nos estudos até agora conhecidos devam ser tratados com algumas precauções, procurando não confundir a ciberdependência com outros tipos de dependências que alguns utilizadores procuram satisfazer através da Internet.

Outro aspecto curioso dos diversos estudos que vão sendo conhecidos, é o tipo de serviços procurados, de acordo com o País. Assim, se nos Estados Unidos, por exemplo, os jogos de apostas são muito procurados, em virtude da sua proibição em muitos dos países, onde essa actividade está ao alcance de todos, esse tipo de serviços não é procurado.

A cibercompulsão é outro tipo de doença, que faz com que a pessoa navegue sem sentido, apenas pelo prazer de navegar, de visitar *sites* onde, na realidade, não adquire nada de novo em termos de conhecimento. Por exemplo, "visita" leilões, *shoppings* ou casinos, o que ainda pode trazer problemas económicos se o adolescente utilizar um número de cartão de crédito.

Vários factores que podem favorecer a cibercompulsão: a acessibilidade, ou seja, a facilidade com que se acede à Internet a um custo cada vez mais baixo; a sensação de autocontrolo que se traduz no sentimento de que se depende unicamente de si, e a excitação, pois cada sessão faz com que o desejo seja maior, o que estimula o doente a "mais e mais". Acresce a ausência de efeitos secundários físicos evidentes, pois os efeitos físicos de uma ciberadicção (problemas oculares, obesidade, má alimentação) não são evidentes senão a longo prazo e o mau rendimento escolar e o isolamento não são suficientemente entendidos como factor de sofrimento.

Sugestão de actividade, se considerar que os mais novos se encontram dependentes da Internet:

Estás dependente da Internet?

Quanto tempo é que costumas passar na Internet? Um par de horas por dia? Mais? O utilizador médio de computador passa 12 horas por semana on-line, mas alguns utilizadores ficam viciados em navegar na Internet. Os psiquiatras chamam a este "ciberpatologia", ou dependência da Internet, e as vítimas não se conseguem separar dos seus computadores. Apresentam sintomas físicos, como por exemplo a agitação psicomotora, secura dos olhos e dores de cabeça, e distanciam-se da família e dos amigos.

Se achas que estás a passar demasiado tempo on-line, podes fazer um teste para concluir qual o teu grau de dependência.

Ligações Úteis

SeguraNet
http://www.seguranet.pt/

Internet Segura
http://www.internetsegura.pt/

Linha Alerta
http://linhaalerta.internetsegura.pt/

Educaunet
http://www.educaunet.org/pt/

Microsoft – Segurança e Privacidade
http://www.microsoft.com/portugal/seguranca/default.mspx

ICRA
www.icra.org

Cybertipline
http://tcs.cybertipline.com/

Netsmartz.org
http://www.netsmartz.org/

Think U Know
http://www.thinkuknow.co.uk/

National Center for Missing and Exploited Children
http://www.missingkids.com/

The United States Children's Online Privacy Protection Act (COPPA)
http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

Testes para verificar o nível de dependência da Internet
http://www.gamblersanonymous.org.uk

Informações sobre a dependência da Internet
http://www.netaddiction.com

Entidades Internacionais de combate ao spam

Antispam.br – Comissão de Trabalho Anti-Spam do Comité Gestor da Internet do Brasil
http://www.antispam.br/

CAUBE - Coalition Against Unsolicited Bulk Email, Austrália
http://www.caube.org.au/

CAUCE - The Coalition Against Unsolicited Commercial Email, América do Norte
http://www.cauce.org/

MAAWG - Messaging Anti-Abuse Working Group
http://www.maawg.org/

Spamcop
http://www.spamcop.net/

The Spamhaus Project
http://www.spamhaus.org/