Módulo 3

Navegar em Segurança

Direitos e Deveres

Índice

1 - Fraudes na Internet

1.1. Comércio Electrónico

O número de utilizadores que fazem compras on-line está a crescer de ano para ano. Em 2006, os consumidores europeus gastaram mais de 100 mil milhões de euros on-line, e alguns analistas consideram que este número deverá aumentar para mais do dobro nos próximos cinco anos. Nas compras mais populares incluem-se os livros, os CD's e as viagens, mas são cada vez mais os utilizadores a comprar vestuário e equipamentos eléctricos on-line.

Comprar on-line é rápido e cómodo, basta um simples clique para comparar os preços de dezenas de lojas virtuais de todo o mundo. E, como as lojas virtuais não têm as mesmas despesas que as lojas tradicionais, os preços são muitas vezes mais baixos.

Ainda existem muitas dúvidas sobre a maneira mais segura de adquirir produtos na Web. Assim, para que esta actividade se realize com segurança é necessário ter alguns cuidados:

- Tente confirmar a fiabilidade do site, se existe de facto uma empresa a representar esse site. Verifique se contém indicações gerais, como o endereço da sede e o número de telefone, e evite aqueles em que não conseguir localizar o vendedor. Em caso de dúvida, antes de efectuar a compra, envie uma mensagem por e-mail pedindo esclarecimentos ou, simplesmente, não compre nesse sítio.

- Tome atenção aos sítios que pedem a indicação do número do cartão de crédito como prova da maioridade do utilizador, mas, na realidade, o usam para lhe debitar automaticamente uma assinatura.

- Ao realizar transacções monetárias na Internet, não faça mais nada até ter terminado. Não abra outras janelas do *browser,* não utilize programas de partilha de ficheiros nem o e-mail.

- Ao aceder à sua conta bancária ou à carteira de títulos on-line, quando terminar a operação não feche simplesmente o *browser,* mas ponha fim à sessão: para isso, clique no botão com a indicação de Sair, Terminar ou outra semelhante.

- Nunca utilize o e-mail para trocar informações respeitantes a pagamentos. Não há problema em receber eventuais confirmações de recepção de encomendas e afins, mas não o use para trocar informações sobre o número do cartão de crédito, da conta bancária, etc.

- Decore as *passwords* e outros códigos, altere-os regularmente e nunca

os guarde no computador pessoal. Na maior parte dos casos, os sítios que se dedicam ao comércio electrónico pedem-lhe para se registar, introduzindo os seus dados pessoais, bem como para escolher um nome de utilizador *(user ID* ou *username)* e uma senha *(password)*. Escolha senhas difíceis de decifrar (evite *passwords* que envolvam o número de telefone, a data de nascimento, etc.) e, se possível, diferentes das que usa para se registar nos sítios de diversão.

- Guarde uma cópia em papel da encomenda e dos *e-mails* trocados com a empresa. Se não receber uma confirmação da encomenda, contacte o vendedor a fim de saber se ele a registou correctamente.

- Ao receber a encomenda, verifique se o produto se encontra em bom estado. Se assim não for, o consumidor tem direito à substituição do produto ou simplesmente a devolvê-lo, sendo, neste caso, reembolsado. Verifique a integridade do produto antes de assinar o documento de recepção.

- Não esquecer que normalmente se pagam despesas de envio. Alguns sites não cobram estas despesas se fizer compras superiores a um determinado montante ou se estiver disposto a esperar alguns dias para que as compras cheguem. A entrega no dia seguinte costuma ser mais dispendiosa. O site deve indicar claramente quanto se irá pagar pelo envio e quando chegará a encomenda.

Compras na União Europeia

Se o site pertencer a uma empresa sediada na União Europeia, será cobrado, consoante o produto, o imposto sobre o valor acrescentado (IVA). Este imposto tem uma percentagem diferente em cada país e é adicionado ao preço base do produto. Algumas lojas virtuais têm os preços dos produtos sem IVA, sendo este apenas adicionado quando se está na página final de pagamento.

A legislação europeia obriga:

- O direito a ter a informação completa sobre o que se compra antes de efectuar a compra;
- O direito a ter uma confirmação por escrito da encomenda;
- O direito de cancelar a encomenda no prazo de sete dias úteis (excluindo fins de semana e feriados) após o pedido;
- O direito a recusar a compra de algo que não se pediu;
- O direito a receber os produtos encomendados no prazo máximo de 30 dias após o pedido de encomenda;
- O direito à protecção contra fraudes com os cartões de crédito.

Compras no estrangeiro

Se uma empresa estiver localizada fora da UE, lembre-se que não tem direito ao mesmo tipo de protecção jurídica e se algo correr mal, pode ser difícil ou mesmo impossível conseguir a devolução do dinheiro.

Quando se fazem compras no estrangeiro, é preciso ter mais alguns cuidados:

- Confirmar se a empresa envia os produtos para Portugal – algumas lojas virtuais dos EUA apenas vendem os seus produtos a pessoas com morada naquele país.
- Tome atenção às despesas alfandegárias e às formalidades de recepção de encomendas de países que não fazem parte da União Europeia – as taxas variam e os custos de envio são provavelmente mais elevados.
- Poderá ter de lidar com unidades de medida diferentes das nossas.

Se Algo Correr Mal

É importante imprimir sempre o pedido de encomenda ou, pelo menos, anotar o que foi pedido e quanto custou. Se algo correr mal, a primeira coisa a fazer é contactar o vendedor e explicar o sucedido, já que pode haver uma solução para o problema. Caso contrário enviar a queixa por escrito para a loja virtual. Se mesmo assim não houver resultados, deverá ser consultada a organização de consumidores ou o Centro Europeu de Consumo, para uma melhor informação dos direitos e até podem intervir e resolver a reclamação.

Se o pagamento foi realizado através do cartão de crédito, deve-se consultar a factura quando receber a encomenda. Se se detectar algo estranho, por exemplo uma taxa de €700 por algo que devia custar €70, deverá contactar a loja virtual a exigir explicações e a rectificação. Se assim não acontecer será oportuno contactar com a entidade emissora do cartão de crédito para bloquearem o pagamento e, se necessário, cancelar o cartão para impedir mais fraudes.

1.2. Leilões On-Line

Na Web existem diversos sites de leilões, com uma grande diversidade de produtos raros e muitas vezes a excelentes preços. No entanto, não se pode esperar o mesmo tipo de protecção jurídica que se consegue em compras efectuadas numa loja virtual. Neste tipo de leilões compra-se directamente a outra pessoa e o site não é obrigado a reembolsar no caso de alguma coisa falhar.

Existem várias leiloeiras *on-line*, por exemplo a famosa leiloeira inglesa Ebay e o Miau em Portugal. Os produtos mais vendidos são, tipicamente, os ligados ao coleccionismo, mas é possível encontrar um pouco de tudo.

Atenção que, nos leilões em geral, não tem as mesmas salvaguardas que existem nas vendas electrónicas normais e não está previsto o direito de reflexão. Assim, é sempre útil adoptar algumas medidas para sua protecção.

- Se o vendedor for um comerciante, o comprador tem os mesmos direitos que em qualquer venda à distância, no que diz respeito a garantias.
- Nunca comunique a sua *password* a ninguém e muito menos o número do seu cartão de crédito. As leiloeiras on-line, nunca enviam mensagens a pedir estas informações, pelo que, se receber alguma, será necessariamente de um impostor.
- Cada utente tem um perfil de *feedback,* isto é, uma classificação global baseada nos comentários emitidos pelos utilizadores. Isto permite controlar a reputação dos vendedores e dos compradores, antes de fazer ofertas.
- Antes de fazer uma compra, leia atentamente os regulamentos e instruções, já que são diferentes de sítio para sítio.

Em caso de dúvida deve-se sempre contactar o vendedor e não esquecer de perguntar qual o valor dos portes de envio. Quanto ao meio de pagamento, convém que seja seguro, do género do MBNet. Se for muito cauteloso, alguns sites providenciam um género de intermediário: envia-se o pagamento para o site do leilão e eles pagam ao vendedor apenas quando receber essa compra.

1.3. Sites falsos e phishing

Análise de Sites

A variedade de tipos de sites é numerosa, cada um especializado num determinado serviço. Os sites podem ser categorizados, por exemplo, quanto ao seu conteúdo:

- Institucionais: servem como ponto de contacto entre uma instituição e seus clientes/fornecedores.
- Mediáticos: são sites informativos com actualizações frequentes e periódicas. Nem sempre o conteúdo é baseado em texto puro, podendo conter variados elementos multimédia, (feeds, RSS) – (como por exemplo: Noticiários, Blogues, Flogs, Podcasts, Vlogs).
- Aplicativos: são sites interactivos cujo conteúdo consiste na utilização de ferramentas de automatização, produtividade e compartilhamento (como por exemplo: processadores de texto, editores de imagem, softwares de correio electrónico, agendas).
- Bancos de dados: servem para catalogar registos e efectuar pesquisas.

- Comunitários: são sites interactivos que servem para a comunicação de utilizadores com outros utilizadores da rede (chats, fóruns, etc.).
- Portais: servem para reunir conteúdos de diversos tipos, geralmente fornecidos por uma mesma empresa/instituição.

Os sites podem, ainda, ser classificados quanto à forma de acesso:

- Abertos: podem ser acedidos livremente.
- Restritos: só podem ser acedidos mediante o pagamento de uma assinatura.
- Por registo: necessitam do preenchimento de um registo gratuito para aceder ao conteúdo.
- Fechados: apenas permitem o registo de pessoas devidamente autorizadas.

A variedade de sites é imensa, assim torna-se fundamental adquirir competências para avaliar os diferentes tipos que encontramos na web.

São cada vez mais os casos de utilizadores da Internet vítimas de sites falsos, criados por criminosos para acederem às suas informações financeiras. No Reino Unido, foram detectados 353 sites falsos de bancos em 2005. Os criminosos atraem os utilizadores aos sites através de *phishing*, ou seja, através de e-mail's que parecem ser de um banco ou de outra empresa pedindo para confirmar o número de cartão de crédito ou outros dados pessoais.

Outras fraudes usuais surgem através de e-mail's com a informação de um prémio e com o pedido de pagamento de uma taxa administrativa antes de o receber; ou e-mail's de um funcionário público estrangeiro a oferecer-se para dividir milhares de euros em troca da utilização da conta bancária para transferir o dinheiro do seu país.

O Instituto do Consumidor alerta para o crescimento deste problema no nosso país. A existência deste fenómeno é cada vez maior, tendo como principal alvo, os bancos.

O que é o *Phishing*?

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.

Como funciona o Phishing?

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 on-line 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.

Que perigos pode apresentar o Phishing?

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.

Cuidados a ter

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 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.

1.4. Publicidade na Internet

Encontramos frequentemente anúncios publicitários em vários formatos no nosso dia-a-dia, até mesmo quando navegamos na Internet. É importante desenvolver competências críticas para analisar os anúncios publicitários e para isso é fundamental ter conhecimento dos vários formatos.

Pop-up

Um dos formatos de anúncios publicitários é o *pop-up*. Este anúncio funciona como uma janela normalmente indesejada, como meio de exibir uma propaganda, com o propósito de chamar a atenção do utilizador. Algumas empresas começaram a desenvolver *software* específico para bloquear janelas de pop-up. Actualmente os browsers permitem bloquear janelas indesejadas. No entanto, os pop-ups continuam a ser desenvolvidos, conseguindo contornar estes softwares.

Spam

Outro dos formatos de anúncios publicitários é o spam, mensagens de e-mail não solicitadas, enviadas em massa. O seu funcionamento já foi referido no Módulo 2.

Banner

O banner é a forma publicitária mais comum na Internet, muito usado na divulgação de sites na Internet que pagam para a sua inclusão. É criado para atrair um utilizador a um site através de um link. Embora todos os tipos de sites sejam susceptíveis a ter banners, são os sites com maior tráfego e conteúdo de interesse que atraem os maiores investimentos de anúncios. A maioria dos utilizadores considera esse tipo de publicidade incómodo porque retira a atenção da página e consome parte da ligação. As últimas versões dos

browsers, incluem opções para desactivar pop-ups ou bloquear os banners. Um outro método para eliminar a presença de banners é utilizar um servidor proxy com o bloqueio activado.

2 – Direitos de Autor

2.1. Validade de fontes

A Internet oferece recursos, mas também contém muita informação que pode não ser útil nem fiável. Dado que qualquer pessoa pode colocar comentários ou informações na Internet, é importante ser capaz de avaliar com precisão a informação que lá se encontra.

Na maioria dos casos, a Internet não dispõe de meios seguros para verificar a validade das informações colocadas on-line. Não esquecer que qualquer pessoa pode criar um sítio Web, sem qualquer tipo de obstáculo. Por isso, verificar, questionar e avaliar a informação que está disponível.

Registamos algumas sugestões para os mais novos relativamente à identificação de informação não fiável:

Sugestões para identificar informações erradas

- Pensa sobre o que encontras quando navegas na Internet. Qual é o objectivo do sítio? Divertir? Vender? O sítio contém informações que possibilitem o contacto com o autor, ou uma secção "Quem somos"? O sítio é patrocinado por alguma empresa, pessoa, ou é um local de conversa público? A Internet é o melhor local para encontrar a informação que se procura?

- Verifica as informações que recolhes on-line, comparando-as com outras fontes. Consulta outros sítios Web ou meios de comunicação social – jornais, revistas e livros – para confirmar a autenticidade da informação.

- Utiliza outros recursos de informação, e não apenas a Internet. As bibliotecas ou as enciclopédias em CD-ROM, permitem-te aceder a fontes de informação alternativas.

- Usa técnicas eficazes de pesquisa de informação on-line, pois isto irá melhorar muito a capacidade de obtenção de informações com qualidade. Uma forma de o fazer consiste em utilizar diversos motores de pesquisa, e não apenas um. Para mais dicas sobre como pesquisar na Internet, pede sugestões aos teus pais ou aos teus professores.

2.2. A legalidade dos downloads

Os direitos de autor conferem ao seu detentor o direito de controlar a realização de cópias e a reprodução de um filme, uma música, uma pintura, etc. Fazer um download sem a permissão do detentor dos direitos de autor, constitui uma ilegalidade. O número de pessoas que fizeram downloads ilegais é tão avultado que é impossível controlar. No entanto, os detentores de direitos de autor estão a tentar encontrar casos que possam servir de exemplo, e isto significa a instauração de acções judiciais.

A indústria cinematográfica tem sido bastante lesada com a partilha de ficheiros. Muitos utilizadores usam software de partilha de ficheiros, e como as ligações à Internet encontram-se cada vez mais rápidas, o download de filmes tornou-se mais fácil. A indústria cinematográfica teme vir a sofrer avultados prejuízos, análogos aos que atingiram a indústria musical nestes últimos anos.

Segundo a Motion Picture Association (Associação da Indústria Cinematográfica), apenas um em cada dez filmes recupera o seu investimento inicial. É necessário reflectir que, nem todos os trabalhadores da indústria cinematográfica ganham milhões de dólares todos os anos.

Actualmente o download de jogos, música, filmes, etc. é uma das actividades mais praticadas pelos jovens na Internet. Esta actividade consiste em transferir da Internet ficheiros de vários tipos para o computador. No entanto, é preciso estar bem informado e atento para não cometer actos ilegais!

2.3. Benefícios e riscos de partilha de ficheiros

Hoje em dia é fácil encontrar e partilhar informação a uma escala mundial. A partilha de ficheiros também designada de peer-to-peer (ou, abreviadamente P2P) tornou-se uma forma prática de partilhar música, áudio, imagens, documentos e software do domínio público, usando para tal os recursos da Internet. Os programas P2P como Morpheus, Kazaa, LimeWire, iMesh e muitos outros, permitem armazenar ficheiros multimédia num espaço específico do computador pessoal e através de uma ligação à Internet possibilitam a partilha de recursos com outros utilizadores que tenham o mesmo software.

Contudo, como acontece com muitas ferramentas poderosas, o software P2P pode ser usado para fins prejudiciais. É importante compreender e estar prevenido em relação aos riscos da partilha de ficheiros P2P antes de dar início a qualquer transferência.

Risco nº1 – Violar as leis de protecção dos direitos de autor

Apesar de haver alguma controvérsia sobre a utilização dos sistemas de partilha P2P para partilhar ilegalmente ou "piratear" material protegido por *copyright*, em particular ficheiros de áudio e imagem, é importante dizer que a utilização de software P2P, devidamente reconhecido, é legal. Todavia, ao usar software P2P, é importante saber distinguir o material sujeito a *copyrights* do material de domínio público. Se tiver dúvidas sobre um determinado ficheiro, o

melhor é não o partilhar ou transferir. Os conselhos seguintes podem ajudar a reduzir estes riscos e a usar o sistema de partilha de ficheiros dentro da legalidade.

Risco nº2 – Expor o computador a software não-desejado

Tal como acontece com a maior parte das coisas que transferimos da Internet, os ficheiros partilhados podem implicar riscos de segurança, como o contacto com vírus, *spyware* e outro software prejudicial. Muito embora a transferência de ficheiros implique sempre algum risco, especialmente quando os ficheiros que transferimos são provenientes de fontes desconhecidas, podemos reduzir os perigos instalando um anti-vírus e um *anti-spyware* e mantendo estas ferramentas activas e actualizadas.

Alguns conselhos para os mais novos relativamente à segurança na partilha de ficheiros:

Conselhos para partilhar ficheiros com maior segurança

- Desconfia de todos os ficheiros e usa software antivírus actualizado para verificar cada ficheiro novo antes de o transferires e reproduzires. Faz regularmente análises ao disco rígido do computador com o software antivírus.
- Apaga o material pirateado que tenhas no teu computador, no leitor de áudio digital, gravadores de CD's ou outros dispositivos de armazenamento. Pensa seriamente em desactivar a opção de transferência do software P2P ou bloquear o acesso exterior do programa, alterando as definições da *firewall*.
- Informa-te bem sobre o software P2P e tenta ser muito cauteloso em relação aos ficheiros que disponibilizas aos outros utilizadores do sistema. A maior parte dos ficheiros partilhados em P2P são normalmente armazenados numa única pasta no computador (muitas vezes intitulada "Os meus ficheiros partilhados", ou semelhante).
- Não guardes cópias de ficheiros sujeitos a *copyright* que tenhas adquirido de forma legal, tal como as músicas de um CD ou as músicas adquiridas num sítio licenciado de venda de música, na pasta do sistema de partilha.
- Faz cópias de segurança dos ficheiros importantes num dispositivo de armazenamento externo, ou num CD-ROM, antes de partilhares ficheiros.

Transferências em Segurança

Mesmo que o computador pessoal esteja bem preparado para a Internet, não há nenhuma tecnologia que o possa proteger contra todos os perigos. E é aí que é necessário saber bem o que se está a fazer. Por isso, antes de se clicar num anexo (ou hiperligação) de uma mensagem de correio electrónico ou de uma mensagem instantânea, antes de se transferir um ficheiro de um sítio Web (ou de uma janela publicitária), ou antes de se partilhar ficheiros com

computadores que não se conhece, é aconselhável ter presente alguns cuidados.

Alguns conselhos para os mais novos relativamente à segurança na transferência de ficheiros:

1. Faz uma pausa antes de abrires ficheiros anexos ou clicares em hiperligações

- Nunca abras anexos em mensagens de correio ou em mensagens instantâneas de estranhos. Se conheces o autor da mensagem, mas se esta for suspeita, confirma a segurança da mensagem com o seu autor. Se não reconheceres o autor, apaga a mensagem de correio electrónico ou ignora a mensagem instantânea.
- Pensa duas vezes antes de clicares em hiperligações que apareçam em mensagens de correio electrónico ou em mensagens instantâneas. O mesmo conselho aplica-se a janelas *pop-up* e a faixas publicitárias. Tem especial cuidado ao clicar nas hiperligações que acompanham um pedido de informações confidenciais, como as que dizem "Clique aqui…"
- Não cliques em botões com o texto "Agree", "OK", "I accept", ou "Concordo", "OK", "Aceito", para te livrares de uma janela publicitária, um aviso inesperado, ou mesmo uma oferta para remover *spyware*. Em vez disso, fecha a janela clicando no botão existente no canto superior direito ou premindo as teclas ALT+F4 no seu teclado.

2. Faz transferências apenas de sítios fidedignos

- Na Internet nem todos os vizinhos são amigos. Evita fazer transferências de um sítio Web ao qual tenhas ido com base na indicação de uma mensagem de correio electrónico enviada por alguém que não conheces. Toma também cuidado caso te depares com um sítio que contenha material censurável, que te faça ofertas que parecem demasiado boas para serem verdadeiras, ou que não inclua uma declaração de privacidade apresentada de forma clara.

3. Respeita a legislação em vigor

- Lembra-te que os textos, música, software, jogos, ou ficheiros de vídeo que se transferem da Internet são o trabalho original de outras pessoas. Os utilizadores que usam material sujeito a *copyright* sem a permissão do seu legítimo proprietário estão a cometer infracções à lei de grande gravidade. A violação da legislação que regula a utilização de tal material pode levar à imposição de multas e mesmo à prisão. Apesar de no passado apenas os grandes infractores serem levados a tribunal, hoje em dia muitos utilizadores domésticos estão a ser sujeitos a acções legais. Além disso, em certos países, é ilegal transferir, ver, ou possuir determinados tipos de dados, como as informações de carácter pornográfico.

4. Instala e usa os programas de partilha de ficheiros com cautela

- Quando usas tecnologias de partilha de ficheiros (também conhecida como peer-to-peer ou P2P) para trocar músicas, vídeos e outros ficheiros na Web, disponibilizas alguns dos teus ficheiros on-line, permitindo que outros usem software semelhante. A utilização de certos programas de partilha de ficheiros pode também implicar deixar o teu computador aberto a ataques enquanto

está ligado à Internet.
- Os programas de partilha de ficheiros têm riscos adicionais. Os programas podem incluir eles próprios software nocivo (ou malware) ou podem mesmo levar a que transfiras conteúdos ilegais, como músicas sujeitas a direitos de autor ou certos tipos de pornografia. E depois de instalados no teu computador, alguns destes programas podem ser difíceis de remover e até mesmo de encontrar!
- Por tudo isto, partilha ficheiros apenas com pessoas que conheces e em quem confias. Alguns utilizadores malfeitores afirmam estar a partilhar música ou filmes, mas na realidade os ficheiros incluem conteúdos perturbadores, vírus, ou elementos mais nocivos.

O que é um Peer-to-Peer?

O Peer-to-Peer, ou P2P ("de par para par," 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.

Como funciona?

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, consequentemente, 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.

Que perigos pode apresentar um Peer-to-Peer?

- **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-chave.

- **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.

Cuidados a ter

- **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.

3 – Telemóveis

O telemóvel é um aparelho de comunicação por ondas electromagnéticas que permite a transmissão bidireccional de voz e dados utilizáveis numa área geográfica que se encontra dividida em células, cada uma delas servida por um transmissor/receptor.

Há diferentes tecnologias para a difusão das ondas electromagnéticas nos telemóveis: a primeira geração (1G) (a analógica); a segunda geração (2G) (existiram melhorias significativas na capacidade de transmissão de dados); a terceira geração (3G) (digital, com mais recursos).

Há vinte anos, as únicas pessoas que tinham telemóveis eram os executivos e os aparelhos eram quase do tamanho de um tijolo. Agora, quase toda a gente tem telemóvel. De acordo com um estudo recente, 70% dos europeus com idades entre 12-13 anos e 23% dos europeus com idades entre 8-9 anos têm telemóveis.

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. Temos pois que assim conhecer bem as funcionalidades dos telemóveis de Terceira Geração, para assim nos podermos proteger de utilizações abusivas e desfrutar de todas as suas vantagens.

Funcionalidades dos telemóveis 3G

Esta secção é dedicada aos os telemóveis 3G, por serem aqueles que permitem a utilização da Internet e a troca facilitada de conteúdos entre dispositivos.

- **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. A tecnologia sem fios Bluetooth® é fornecida com muitos telemóveis e PDAs. Inicialmente concebida para permitir a troca de

documentos entre outros dispositivos Bluetooth sem a utilização de cabos de ligação, expandiu-se desde então para fornecer outros serviços, tais como conectividade Web e jogos on-line.

- **Acesso à Internet** – Uma das novidades dos telemóveis 3G é poderem (quando equipados para tal) aceder à Internet. Tal como um computador, um telemóvel poderá aceder ao e-mail, aos chat's 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.

- **SMS e MMS** - O envio de mensagens escritas, de imagem, som e vídeo para as redes móveis é uma actividade cada vez mais utilizada, quer pelos jovens quer pelos adultos, nos dias de hoje. As mensagens de texto são mais baratas do que as chamadas, mas podem ser viciantes – alguns psicólogos consideram que são mais susceptíveis de criar dependência do que a Internet. Pensa-se que a primeira pessoa a receber tratamento devido a uma dependência de mensagens de texto foi um jovem de 19 anos da Escócia. Gastou 6 600 euros em mensagens de texto num ano, e houve uma altura em que enviava cerca de 700 mensagens por semana.

Que perigos pode apresentar um telemóvel?

Um telemóvel, tal como os computadores, também é vulnerável a certos perigos, como os do phishing, SPAM, roubo de identidade e cyberbullying, pelo que se aplicam algumas regras:

- **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 mensagen (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** – 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. Quando está no modo "visível", o telemóvel ou PDA bluetooth envia um sinal a indicar que está disponível para "emparelhar" com outro dispositivo bluetooth e transmitir e receber dados. No entanto, um intruso que detecte este sinal poderia igualmente tentar emparelhar com o seu dispositivo e aceder ilicitamente aos seus dados, para roubar o seu número de identificação pessoal (PIN). Poderá não ter a noção que o intruso, com o seu PIN, poderá roubar informações guardadas no seu dispositivo, incluindo listas de contactos, mensagens de correio electrónico e mensagens de texto;Enviar mensagens de texto ou imagens não solicitadas para outros dispositivos Bluetooth; Aceder aos comandos do seu telemóvel , o que permitiria que o intruso utilizasse o seu telemóvel para fazer chamadas, enviar mensagens de texto, ler e escrever contactos na lista telefónica, escutar conversas e ligar à Internet; Instalar um vírus no seu dispositivo, que poderia provocar os mesmos danos que um vírus de computador — por exemplo, abrandar ou desactivar o seu serviço, ou destruir e roubar informações; os criminosos também andam com detectores Bluetooth, à procura de telemóveis e PDAs para infiltrar, instalando potentes antenas em computadores portáteis, de forma a captar sinais Bluetooth a uma distância até perto de um quilómetro.

- **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.

Cuidados a ter

Algumas regras básicas 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.

- **Mantenha a definição Bluetooth para "não visível" –** Deixar o telemóvel ou PDA no modo visível faz com que esteja perigosamente aberto a transmissões Bluetooth— um utilizador Bluetooth a uma distância de 9 metros pode receber o seu sinal e utilizá-lo para aceder ao seu dispositivo enquanto você anda na rua, conduz, ou mesmo trabalha no seu escritório. Utilize um código PIN robusto. Os códigos de cinco dígitos ou mais são difíceis de descodificar. Evite guardar dados sensíveis, tais como o seu número de segurança social, números de cartões de crédito e palavras-chaves em qualquer dispositivo sem fios. Mantenha-se actualizado sobre as evoluções e problemas de segurança da tecnologia Bluetooth e consulte regularmente o fabricante do seu dispositivo para conhecer as actualizações de software ou quaisquer vulnerabilidades de segurança específicas.

- **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 edóneas. 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.

PDA's

Os PDAs (**Personal digital assistants)**, são computadores de reduzidas dimensões, cumprindo as funções de agenda e computador com funções básicas, com a possibilidade de ligação a um computador pessoal e uma rede informática sem fios para acesso à Internet, tendo ainda alguns a capacidade de realizar chamadas telefónicas.

Existem três famílias principais de PDAs no mercado: Os PalmOne, os Pocket PC e os Pocket Linux.

O número de PDAs no mundo vem crescendo de forma exponencial, mas tendências indicam que em poucos anos os Smartphones (desenvolvido através da "fusão" entre um PDA e um telemóvel) serão maioria absoluta.

Actualmente os PDAs permitem realizar um sem número de tarefas. Desde tocar mp3 , mostrar vídeos, tirar fotos, funcionar com GPS, etc.

Ameaças à medida

São já muitos os vírus escritos especificamente para tirar partido dos PDAs. Por conseguinte, é aconselhável investir num programa antivírus para o seu dispositivo em versão móvel.

As ligações via Wi-FI, Bluetooth, devem ser efectuadas de acordo com regras de segurança básicas: não acedendo a ligações estranhas e não aceitando ficheiros desconhecidos.

4 – Consolas

As consolas permitem a participação numa variedade de jogos e actividades, alguns dos quais pela Internet. De forma que, a questão da segurança on-line também se coloca. Destacamos as recomendações de segurança fornecidas pela Nintendo na utilização da consola Wii.

Pais – Proteger a privacidade dos seus filhos

- Antes de deixar os seus filhos utilizarem a consola Wii, recomendamos vivamente que lhes explique a importância de não partilharem qualquer informação pessoal com desconhecidos. Informe-os de que não devem usar nenhuma informação pessoal nos nicknames na consola Wii, nos nomes de utilizador das salas de chat, nos nomes dos Miis ou quaisquer outros aspectos dos Serviços oferecidos através da consola Wii. Explique-lhes o perigo de receberem mensagens de desconhecidos ou da comunicação com desconhecidos.
- Deve vigiar as crianças sempre que estas utilizarem a consola Wii e ajudá-las na configuração da consola Wii. Se, em qualquer altura, pretender que os seus filhos deixem de usar as características interactivas ou on-line da consola Wii, pode restringir o acesso aos serviços on-line da Wii utilizando o Controlo Parental.

Proteger a privacidade da sua informação pessoal quando utiliza a consola Wii

- Nunca divulgue informações pessoais, tais como o seu primeiro e último nome, número de telefone, data de nascimento, idade, endereço electrónico ou morada, quando comunicar com desconhecidos ou usar qualquer um dos serviços oferecidos na sua consola Wii.
- Se utilizar as funções de mensagem da consola Wii, deve ter em conta que a Nintendo pode controlar a sua utilização e partilha de informação (i) como previsto na lei (ii) quando necessário para proteger a sua empresa, clientes e empregados ou (iii) quando necessário para fornecer os seus serviços.
- Se decidir fornecer informações pessoais a outros sites da Internet, a partilha dessa informação estará sujeita à política de privacidade dessa empresa, e não às políticas de privacidade da Nintendo. Seja prudente ao fornecer qualquer informação pessoal a terceiros através dos serviços de rede oferecidos na sua consola Wii.
- A sua consola Wii pode guardar determinada informação pessoal no seu Comando Wii, por isso tenha em atenção que ao usar o Comando Wii noutra consola que não seja a sua, é possível que determinada informação pessoal seja partilhada com essa consola.
- Para sua protecção, antes de vender, dar ou de algum modo transferir a sua consola Wii, por favor certifique-se que limpou e removeu da sua consola

Wii, de forma segura, toda a sua informação pessoal, incluindo fotografias ou mensagens do Quadro de Mensagens da Wii e toda a informação sensível armazenada no disco duro da consola Wii.

Alguns itens adicionais a considerar

- Ao decidir se um jogo é apropriado para o seu filho, verifique a classificação da idade. Utilize a classificação para seleccionar o jogo mais apropriado para o seu filho.
- Considere a personalidade única do seu filho, o nível de maturidade e capacidades. Todas as crianças são diferentes e os pais devem usar o bom senso ao escolherem quais os jogos apropriados para as suas crianças.
- Utilize o Controlo Parental fornecido. O Controlo Parental limita o acesso do seu filho a certos jogos e funções da Wii.
- Jogue com os seus filhos. Veja que jogos os seus filhos estão a jogar e fale com eles sobre os jogos e outras coisas sempre que possível. Nunca terá demasiado conhecimento sobre os jogos que os seus filhos estão a jogar.
- Não pare nas classificações. Procure na Internet e nas revistas entusiastas de jogos por críticas a jogos nos quais as suas crianças estejam interessadas.

Precauções de Segurança

Sabemos que a segurança e o bem-estar dos seus filhos são muito importantes para si. Apesar de jogar videojogos ser uma actividade geralmente segura, é boa ideia estar informado sobre as precauções de segurança que deve ter para si e para a sua família enquanto utilizam a consola. A Wii introduz uma maneira totalmente nova de jogar e de desfrutar dos jogos. O Comando Wii oferece controlo intuitivo a qualquer pessoa que utilize o movimento físico. Os jogadores ficam concentrados no jogo fazendo os movimentos necessários para controlar a sua personagem no ecrã. Se está a jogar baseball, utiliza o mesmo movimento como se baloiçasse o bastão para bater a bola; no ténis, o movimento é o de um jogo de ténis real; lutas de espadas imitam o movimento de verdadeiras lutas com espadas.

Por isso, é importante os pais vigiarem os seus filhos num jogo apropriado. Os jogadores devem fazer intervalos de 10 a 15 minutos em cada hora, mesmo que pensem que não precisam. Se, com os movimentos físicos adicionais, sentir as mãos, pulsos, braços ou olhos ficarem cansados ou doridos enquanto joga, ou se tiver sintomas como formigueiro, torpor, queimaduras ou rigidez, deve parar de jogar e descansar durante algumas horas antes de voltar a jogar.

http://wiiportal.nintendo-europe.com/16867.html

Normas específicas de segurança para a utilização de outras consolas:
Playstation – Sony - http://pt.playstation.com/help-support/
XBox – Microsoft – http://www.xbox.com/pt-PT/legal/privacystatement.htm

Os videojogos, especialmente os que dispõem de opções de utilização on-line ou multijogador, são tão ou mais apelativos do que a televisão, a música e os filmes para crianças, jovens e adultos. É essencial obter informação sobre a comunidade de jogos, as classificações dos jogos e sobre como utilizar as ferramentas de privacidade e segurança incluídas nos jogos, de forma a ajudar a manter a segurança dos jovens nos jogos. Assim, quando os jogos são adequados à faixa etária, tornam-se interessantes, divertidos, e mesmo educativos.

Do guia de pais, foram retiradas algumas sugestões básicas sobre como pode tomar decisões informadas para ajudar a proteger os jovens e as crianças quando jogam e competem on-line.

- **Informe-se.** Familiarize-se com as classificações dos jogos e as declarações de privacidade, e veja os termos de utilização aceitável de todos os sites de jogos on-line.

- **Observe.** Veja quais os jogos que os seus filhos jogam e com quem jogam. Coloque o computador ou a consola de jogos num local onde possa monitorizar facilmente a actividade e interesse-se pelos jogos que os seus filhos jogam.

- **Estabeleça regras.** Deve estabelecer regras antes de o seu filho iniciar jogos on-line e certificar-se de que ele as compreende. As regras típicas incluem: limitar o tempo que pode passar a jogar, jogar apenas com amigos off-line, nunca conversar com desconhecidos e nunca revelar informações pessoais, o que inclui o nome real da criança e o local onde vivem.

- **Monitorize conversas e mensagens.** Se um jogador utilizar linguagem inadequada, encoraje o seu filho a dizer-lhe que tal aconteceu, para tentar seleccionar o nome da pessoa em questão na lista de jogadores e silenciar ou bloquear as suas mensagens, ou denunciá-los aos administradores do jogo, através de correio electrónico, chat, ou secções de feedback. Consulte o site de jogos em questão para obter mais informações.

- **Assegure a privacidade.** Aconselhe os seus filhos a nunca revelarem informações pessoais (por exemplo, o nome, a idade, o sexo, ou o endereço de casa), mostrarem fotografias deles, ou aceitarem conhecer alguém pessoalmente, quando utilizam salas de chat. Certifique-se de que sabem que devem informá-lo imediatamente no caso de alguém lhes pedir este tipo de informações.

- **Utilize a conversação por voz (voice chat) de forma sensata.** Alguns sistemas de jogos permitem-lhe utilizar um conjunto de auscultador e microfone para conversar com outros jogadores. (Tal não é recomendado para as crianças mais novas.) Consulte o manual do seu computador ou da sua consola de jogos, para obter mais informações

sobre esta característica.

- **Escolha nomes adequados.** Certifique-se de que o seu filho escolhe bem os nomes de ecrã ou de personagem (também chamados gamertags), respeitando as regras do site de jogos. Estes nomes não devem ser reveladores de nenhuma informação pessoal, ou ser um convite potencial a assédio.

- **Tenha cuidado com o assédio on-line.** Saiba como lidar com utilizadores que usam a intimidação em jogos on-line (também conhecidos como griefers ou cyberbullies).

- **Ensine hábitos de segurança no ciberespaço aos seus filhos.** Diga aos seus filhos que se sentirem pouco à vontade com alguma coisa que se esteja a passar num jogo, devem parar de jogar e informá-lo sobre esse facto de imediato, para que possa registar e comunicar o problema, se tal for necessário.

- **Participe.** Uma das formas mais seguras de os seus filhos jogarem on-line consiste em jogar com eles. Esta poderá ser a última coisa que eles querem, especialmente se já forem um pouco mais velhos, mas é uma boa forma de os ajudar a aprender a lidar com as outras pessoas on-line, ao mesmo tempo que continuam a divertir-se.

Ligações Úteis

SeguraNet
http://www.seguranet.pt/

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

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

Deco – Comércio Electrónico
www.deco.proteste.pt

Unicre – Comércio Electrónico
www.unicre.pt

AIP – Comércio Electrónico
www.estudar.org/eCommerce

Observatório do Comércio – empresas portuguesas aderentes ao comércio electrónico
www.Obscom.min-economia.pt

Consumer Direct – Fraudes na Internet
http://www.consumerdirect.gov.uk

Direcção-Geral do Consumidor
http://www.consumidor.pt/

APWG – Reportar situações de fraude na Internet
www.antiphishing.org