

- 1) Guia de utilização de Internet Regras Básicas de Segurança na Utilização de um computador público.**
- 2) Guia de Utilização de Internet de Regras Básicas de Segurança Anti-Spyware.**
- 3) Guia de Utilização de Internet de Regras Básicas de Segurança no Acesso ao Correio Electrónico.**
- 4) Guia de Utilização de Internet de Regras Básicas de Segurança de Segurança para crianças e Jovens.**
- 5) Guia de Utilização de Internet de Regras Básicas de Segurança para Pais.**
- 6) Guia de utilização de Internet Regras Básicas de Segurança em Salas de Conversação – Chat e Redes Sociais.**
- 7) Guia de Utilização de Internet, endereços de alguns sites onde se pode descarregar programas para filtrar e ou limpar informação não desejada.**
- 8) Guia de Utilização de Internet, ferramentas que podem ajudar os pais a obstruírem o acesso de informação não desejada e podem ser agrupados pelas seguintes características.**
- 9) Guia de Utilização de Internet, sites onde encontra informações úteis sobre segurança de crianças e jovens na Internet**
- 10) Glossário de termos informáticos úteis**

1) Guia de Utilização de Internet e Regras Básicas de Segurança na Utilização de Um Computador Público

Sugestões para uma utilização mais segura

➤ Não guarde as suas informações de início de sessão

Muitos programas (especialmente programas de mensagens instantâneas) incluem funcionalidades de início de sessão automático que guardam o seu nome de utilizador e a sua palavra -passe. Desactive esta opção para que ninguém possa iniciar uma sessão com os seus dados;

➤ Como desactivar a funcionalidade que guarda todas as palavras – passe?

Deve deixar a caixa de memorização da password em branco;

➤ Não saia do computador se este contiver informações importantes no ecrã.

Se tiver de sair do computador público, termine a sessão em todos os programas e feche todas as janelas que possam apresentar informações importantes.

Elimine o histórico da internet. Os WEB Browsers, como o Internet Explorer, mantêm um registo da palavra -passe e de cada página que visita, mesmo após ter fechado as páginas e ter terminado a sessão;

➤ Tenha em atenção os olhares sobre o ombro

Ao utilizar um computador público, tenha especial atenção a pessoas podem tentar espreitar por cima do seu ombro ou ver enquanto introduz a palavras -passe, de forma a ter acesso à sua informação;

➤ Não introduza informações importantes num computador público.

Tenha em atenção que pode ter sido instalado software sofisticado no computador público, que regista cada operação do teclado e que envia por correio electrónico a sua informação.

Nestes casos não tem importância se não guardou as suas informações ou se eliminou os seus registos. Os piratas informáticos continuam a ter acesso a estas informações.

Por isso, evite digitar o número do seu cartão de crédito em computadores públicos;

➤ Regras para criação da palavra - passe

- Password complexa mas fácil de fixar;
- Utilize preferencialmente 8 caracteres com maiúsculas, letras e números e caracteres especiais como exemplo, os símbolos !, ?, =

➤ Como eliminar os ficheiros temporários(Cookies)

Para eliminar todos os cookies, siga estes passos:

- No Internet Explorer, clique no botão **Ferramentas** e, em seguida, clique em **Opções da Internet**.

- No separador **Geral**, em **Histórico de navegação**, clique em **Eliminar**.
- Seleccione a caixa de verificação **Cookies** e, em seguida, clique em **Eliminar**

➤ **Como Eliminar o histórico de navegação**

- No Internet Explorer, clique no botão **Segurança** e, em seguida, clique em **Eliminar Histórico de Navegação**.
- Seleccione a caixa de verificação junto a cada categoria de informação que pretende eliminar.
- Seleccione a caixa de verificação **Manter dados dos Web sites Favoritos**, se não pretender eliminar os cookies e ficheiros associados aos Web sites da sua lista de Favoritos.
- Clique em **Eliminar**. Esta operação pode ser demorada se tiver muitos ficheiros e histórico.
- Quando elimina o histórico de navegação, a lista de favoritos ou os feeds subscritos não são eliminados
- Pode utilizar a funcionalidade Navegação InPrivate do Internet Explorer para evitar deixar um histórico à medida que navega na Web.

➤ **Como alterar o número de dias que as páginas Web são mantidas na histórico de Navegação**

- No Internet Explorer, clique no botão **Ferramentas** e, em seguida, clique em **Opções da Internet**.
- Clique no separador **Geral**.
- Em **Histórico de navegação**, clique em **Definições**.
- Em **Histórico**, especifique o número de dias que deseja que o Internet Explorer utilize para recordar as páginas Web visitadas. Se não quiser manter o histórico de páginas Web, defina o número de dias com 0.
- Clique duas vezes em **OK**.

➤ **Para maior segurança navegue em InPrivate**

O que é a Navegação InPrivate?

O Internet Explorer 8 inclui o novo complemento “InPrivate”

A Navegação InPrivate permite-lhe navegar na Web sem deixar rasto no Internet Explorer. Isto ajuda a impedir qualquer pessoa que utilize o computador posteriormente de ver o que visitou e o que viu na Web. Pode iniciar a Navegação InPrivate com a página Novo Separador, clicando em “Abrir uma janela de navegação InPrivate”

Ao iniciar a Navegação InPrivate, o Internet Explorer abre uma nova janela. A protecção que a Navegação InPrivate proporciona só está activa enquanto consulta essa janela. Pode abrir os separadores que quiser nessa janela, pois estes serão protegidos pela funcionalidade Navegação InPrivate. No entanto, se abrir uma janela de outro browser, essa janela não será protegida. Para terminar a sua sessão de Navegação InPrivate, feche a janela do browser.

Enquanto estiver a navegar utilizando a Navegação InPrivate, o Internet Explorer guarda algumas informações, tais como cookies e ficheiros temporários da Internet para que as páginas Web que visitar funcionem correctamente. No entanto, no final da sessão de Navegação InPrivate estas informações são eliminadas.

2) Guia de Utilização de Internet e Regras Básicas de Segurança Anti-Spyware

O spyware é um software que pode apresentar anúncios (tais como janelas de publicidade), recolher informações acerca do utilizador ou alterar definições no computador, geralmente, sem o seu consentimento. O spyware pode ser instalado por Web sites, programas transferidos ou por programas instalados a partir de CD-ROM ou disquete. O spyware é instalado, sobretudo, através de software gratuito, tal como software para partilha de ficheiros, protecções de ecrã ou barras de ferramenta de procura.

Como distinguir se tem spyware no computador?

➤ ***O computador está a funcionar muito lentamente?***

É um sintoma que o computador tem vírus. No entanto, podem existir outras razões para um desempenho lento, que podem incluir um disco rígido que necessita ser desfragmentado, ou o computador necessita de mais memória (RAM) ou a existência de spyware.

➤ ***O modem ou disco rígido está a funcionar sem parar?***

Os vírus de correio electrónico funcionam enviando múltiplas cópias de si próprios através de correio electrónico. Um indicador desta situação é a luz de actividade no modem de banda larga ou externo estar constantemente acesa; um outro indicador é ouvir continuamente som do disco rígido em funcionamento. Estes nem sempre são sintomas de um vírus de computador, mas quando combinados com outros problemas, poderão indicar uma infecção por vírus.

➤ **Estão a ser apresentadas mensagens de erro inesperadas ou os programas estão a ser iniciados automaticamente?**

Alguns vírus podem provocar danos no Windows ou nalguns dos programas. Os resultados desta situação podem incluir a apresentação inesperada de mensagens, programas que são iniciados ou fechados automaticamente ou o Windows encerrar repentinamente.

➤ **Como evitar que o Spyware infecte o computador?**

instalar um programa anti-spyware, assim como manter o Windows actualizado e as definições de segurança do Internet Explorer nos níveis recomendados, minimizando a ameaça;

Quando visita Web sites, não concorde automaticamente em transferir algo que o site ofereça. Se transferir software gratuito, tal como programas para partilha de ficheiros ou protecções de ecrã, leia o acordo de licença cuidadosamente. Procure cláusulas que obrigam a aceitar anúncios e janelas de pop-up da empresa, ou que indiquem que o software irá enviar determinadas informações para o fabricante do software.

Vantagens na utilização de software anti-spyware:

Os programas antispyware são frequentemente incluídos nos produtos antivírus. Se já tiver um produto antivírus instalado, verifique se este inclui as capacidades de antispyware ou se poderá actualizar o produto para as acrescentar e, em seguida, execute a verificação. Se não tiver uma ferramenta antispyware, poderá obter várias a partir da Internet. Escolha uma de uma origem fidedigna ou peça uma recomendação a alguém.

Exemplos de software anti-spyware (gratuito):

➤ **Windows Defender**

O Windows Defender é um programa gratuito que ajuda a proteger o computador contra pop-ups, baixa performance e ameaças de segurança causadas por spywares e outros softwares maliciosos. Fornece protecção, um sistema de monitorização que recomenda acções em spywares quando são detectados e minimiza interrupções, ajudando a manter o computador operacional. O programa está na versão final e é suportado pelo Windows XP

Na página sobre segurança do site da Microsoft Portugal

<http://www.microsoft.com/Portugal/seguranca>

Na barra lateral esquerda clicar em “segurança em casa” e depois em “spyware”

- *Lavasoft Ad-ware* www.Lavasoft.com detecta e remove facilmente spywares do sistema e protege o computador
- www.download.CNET.com

3) Guia de Utilização de Internet e Regras Básicas de Segurança de Acesso ao Correio Electrónico

Algumas das ameaças que os utilizadores de e-mail estão sujeitos:

- A multiplicação do uso do e-mail como forma de divulgação não solicitada e/ou indevida;
- Recepção de spam (pelo menos 80% do que circula hoje por e-mail é spam);
- A entrada dos vírus faz-se sobretudo através de e-mail, tanto de forma visível como alojando-se no computador e é despoletado em datas determinadas, ex. 25 de Dezembro, 1 de Janeiro;
- O roubo de identidade faz-se através de e-mails fraudulentos como inquéritos

Consequências:

➤ **Revelar Informação**

Vírus propagados por correio electrónico copiam endereços de correio electrónico dos livros de endereços ou ficheiros encontrados no sistema infectado. Alguns vírus também tentarão enviar ficheiros de uma máquina infectada para outros potenciais vítimas ou até para o autor do vírus. Estes ficheiros podem conter informação sensível;

➤ **Adicionar/Modificar/Apagar ficheiros**

Uma vez comprometido o sistema, um vírus pode potencialmente adicionar, modificar ou apagar ficheiros nesse sistema. Estes ficheiros podem conter informação pessoal ou ser necessários para o bom funcionamento do sistema informático;

➤ **Afectar a estabilidade do sistema**

Os vírus podem consumir quantidades consideráveis de recursos computacionais, fazendo com que o sistema se torne lento ou até inutilizável;

➤ **Instalação de uma “backdoor”.**

Muitos vírus podem instalar uma “backdoor” no sistema infectado, que pode ser usada remotamente por um Hacker, para conseguir acesso, ou para adicionar/modificar/apagar ficheiros no sistema;

➤ **Enviar correio electrónico não solicitado em massa (SPAM) a outros utilizadores**

Muitas vezes os “spammers” utilizam sistemas comprometidos para enviar correio electrónico em massa. São computadores que não estão protegidos para utilização “final” (ex. sistemas domésticos e de pequenas empresas);

Sugestões para uma maior segurança

- Não abra mensagens de origem desconhecida;
- Não abra mensagens que alertem para um vírus muito grave e que contenha um ficheiro em anexo, para efectuar a limpeza, este normalmente contém vírus;
- Não abra, anexos ou clique em links de origem desconhecida;

- Não descarregue, execute, ou corra programas sem ter a certeza absoluta que este é da autoria de uma pessoa ou empresa em que confia;
- Tenha cuidado com os URLs nas mensagens de correio electrónico. Os URLs podem conduzir a conteúdos maliciosos que, em certos casos, podem ser executados sem intervenção do utilizador. O hacker utiliza URLs para que os utilizadores acedam a “web sites” maliciosos. Estes “sites” simulam “sites” legítimos, de modo a solicitar informação sensível tal como palavras-chave ou números de contas;
- Tenha cuidado com as mensagens onde é solicitado o preenchimento de dados pessoais e o seu reenvio. Analise se a sua origem é fiável e de segurança (por exemplo se foi enviada por uma instituição credível e certificada. Ex. inquéritos falsos das Finanças que visam obter dados de forma fraudulenta);
- Não compre produtos de empresas que se apresentam em e-mails de spam (os spammers costumam trocar ou vender endereços de e-mail dos clientes);
- Quando enviar uma mensagem para mais do que uma pessoa, não envie no campo “Para” nem no campo “Cc”, envie em “Cco” ou “Bcc”, assim evita que sejam visíveis os endereços electrónicos aos Hackers. Quando reenviar mensagens, retire os nomes e endereços dos e-mail por onde já circularam;
- Não reencaminhe “**correntes de e-mail**” recebidas em mensagens de e-mail (a maioria das vezes somos sugestionados a enviar para terceiros mensagens com avisos e informação falsa);

4) Guia de Utilização de Internet e Regras Básicas de Segurança para Crianças e Jovens

Sugestões para quando navegas na Internet.

- A origem (site) da informação é essencial, compara com outras fontes onde podes encontrar essa mesma informação (livros, jornais, revistas, televisão, rádio, amigos, pais ou colegas) ;
- Conta aos teus pais e/ou professores se encontrares informação ou imagens que te incomodem: pornografia, apelo à violência, apelo ao racismo, ou outras situações;
- Tem cuidado com os vírus que podem ser descarregados para o teu computador quando acedes a jogos na internet ou quando descarregas determinados programas. O mesmo pode acontecer com e-mails enviados por desconhecidos;
- Se receberes e-mails suspeitos, arquivos ou fotos de alguém que não conheces, remove-os. Evita clicar nas URLs que parecem suspeitas ;
- Deves respeitar a propriedade dos outros. Fazer cópia ilegal do trabalho de outras pessoas, tem uma pena até 3 anos de prisão;
- Quando utilizares textos de outras pessoas deves colocar entre “aspas”, e colocar o nome dos autores entre parênteses rectos.

Cuidados a ter na comunicação através de e-mail, chat ou MSN.

- Tem cuidado quando estás em salas de chat e não conheces quem está no outro computador. Nunca te encontres pessoalmente com essas pessoas, muito menos sozinho. Na Internet nunca se tem a certeza com quem conversamos. O teu amigo pode ser um adulto perigoso;
- Não converses com ninguém que conheceste on-line sobre algum problema pessoal, tenta falar com os teus pais, parentes ou amigos. Eles são um recurso melhor, mais confiável que um estranho, embora possas sentir-te mais á vontade, uma vez que não o conheces;
- Nunca divulgues informações sobre tua vida, como por exemplo, o teu nome completo (utiliza apenas um nick-name, pseudónimo), morada, telefone, onde vives, ou onde é a tua escola. Desconfia daqueles que querem saber muito sobre ti, pois mesmo com poucas informações as pessoas podem descobrir onde moras, ou a escola que frequentas;
- Não envies fotografias tuas, nem da tua família;
- Tem cuidado com a utilização da Webcam com pessoas que não conheças;
- Nunca dêes a tua password a ninguém;
- Nunca faças compras on-line sem conhecimento dos teus pais;
- Se te insultarem, não respondas. Mantém um comportamento ético e de boas maneiras quando comunicas com alguém. Nunca envies mensagens ofensivas ou desagradáveis. Lembra-te que o que escreveres ou enviares, pode ser reenviado a outras pessoas, até mesmo aos teus pais ou para a tua escola;
- Se alguém com quem estiveres a conversar, disser ou enviar algo que te faça sentir desconfortável ou com medo, desliga o computador. Se não tiveres fornecido informações tuas, a pessoa não poderá

ameaçar-te, simplesmente podes ignorar a pessoa (ou bloqueá-la) no futuro. Avisa aos teus pais ou os professores se continuares a sentir-te com medo ou ameaçado;

- Bloqueia e apaga contactos em caso de CyberBullying;

O que é o CyberBullying?

O bullying consiste numa perseguição constante de crianças mais velhas ou fortes a crianças mais novas ou fracas, traduzindo-se numa perseguição constante a um (ou vários) elemento de um grupo.

O CyberBullying consiste no desenvolvimento destas actividades recorrendo às ferramentas disponíveis na Internet.

Neste campo, as Redes Sociais fornecem algumas ferramentas aos perseguidores uma vez que lhes dão meios para concretizarem, as suas acções :

- Facilidade de ataque através de comentários pouco abonatórios e constantes no perfil do alvo;
- Revelação de segredos ou imagens embaraçosas On-line;
- Exclusão premeditada de alguém de um grupo;
- Ameaças físicas;
- Facilidade em manter o anonimato, criando um perfil falso;
- Facilidade em divulgar comentários num grupo específico e restrito (Ex: escola);
- As Redes Sociais fornecem todas as ferramentas geralmente utilizadas nestes ataques num único interface: Mensagens Instantâneas, SMS, perfis falsos e caluniosos, difusão controlada de mensagens caluniosas;

5) Guia de Utilização de Internet e Regras Básicas de Segurança para Pais

A Internet é uma ferramenta de informação útil para apoiar a aprendizagem, e o lazer. Enquanto meio de comunicação e de informação de livre acesso tem alguns riscos a que os pais devem ter em atenção.

Sugestões

- Verifique o tipo de acesso a comunicações electrónicas *On-line* - salas de conversação, Fóruns, Mensageiros (Instant Messenger) seu correio electrónico ou programas tipo P2P (Peer to Peer) que os seus filhos têm acesso;
- Limite os tempos de acesso à Internet e não os deixe consultar pelo menos 2H antes de se deitarem. Quase sempre os aliciadores entram em contacto com as suas possíveis vítimas nas salas de conversa. Depois de conhecerem um menor através do computador, continuam a comunicar através do correio electrónico (e-mail);
- Consulte o Histórico da Internet;
- Converse com os seus filhos sobre os sites que visitam na Internet e sobre os diálogos que mantêm através de e-mail, chat, Messenger, e explique-lhes o perigo a que estão expostos;
- A Internet mal utilizada é espaço privilegiado para ofertas enganosas e aliciamento encoberto, Em caso de suspeita salve todos os elementos relativos à proveniência e conteúdos dos contactos;
- Alerta os seus filhos para o risco de comunicar com estranhos, os "amigos" on-line são na realidade, estranhos.
Alerte-os para que não forneçam dados pessoais (nome completo, morada, telefone, passwords...) e não marquem encontros com quem não se conhece;
- Coloque o computador numa divisão comum da casa, para evitar o isolamento do seu filho, de forma a não estar sozinho. O computador no quarto também não é saudável, porque tem campos electromagnéticos;
- Alerta o seu filho para as fontes de informação na Internet e a comparar diversas fontes, à semelhança do que acontece em relação aos restantes Media (televisão, rádio jornais, revistas);
- Aconselhe os seus filhos a manter um comportamento ético quando pesquisa na Internet. Deverá respeitar os *Direitos de Autor* referindo o local (Site) ou autor de onde foi retirada a informação (imagem e texto);
- Aconselhe os seus filhos a não responderem a provocações, quando estiverem a comunicar através de e-mail, chat ou Messenger, este tipo de diálogo não deve ser alimentado, aconselhe-o a desligar a Internet quando isso acontece;
- Alerta os seus filhos para os perigos dos vírus que podem introduzir-se nos computadores, ao abrirem e-mails e anexos estranhos ou enviados por desconhecidos, ou ao descarregar determinados programas da Internet. Actualize o antivírus, diariamente, ou sempre que vai à Internet antes de consultar qualquer site;
- Poderá também instalar software de filtragem de conteúdos, de modo a evitar o acesso a sites ofensivos ou ilegais;
- Alerta os seus filhos para os perigos da pirataria (3 anos de prisão) jogo a dinheiro, conteúdos ilícitos, ameaças, extorsão, partilha e transferência de ficheiros de música e vídeo não

autorizados pelos autores;

- Recomende aos seus filhos que não façam compras na Internet sem a sua autorização. Poderá correr riscos ao dar o seu número de cartão de crédito. Recomendamos que se for usual fazer compras online, peça um MBNET (cartão virtual de saldo controlado) só para compras;

6) Guia de Utilização de Internet e Regras Básicas de Segurança em Salas de Conversação (Chat) e Redes Sociais.

Os Chats e as Redes sociais são serviços que têm como objectivo o estabelecimento de ligações entre utilizadores que se conhecem ou que partilham interesses ou actividades comuns, permitindo trocas de experiências, vivências e conhecimentos entre os vários utilizadores. São locais virtuais na Internet em que as pessoas podem escrever mensagens que surgem quase imediatamente nos computadores das outras pessoas com quem se está a conversar on-line. Principais riscos a que todos os utilizadores deste tipo de serviço devem estar atentos, bem como algumas precauções que podem ser tomadas para os minimizar. Existem actualmente diversos serviços, sendo uns são mais focalizados num aspecto, como acontece com o LinkedIn (<http://www.linkedin.com/>), em que o principal objectivo são as relações profissionais, o Myspace é mais generalistas, (<http://www.myspace.com>), assim como o Facebook (<http://www.facebook.com>) ou o hi5 (<http://www.hi5.com>), entre outros. Estes serviços permitem, fundamentalmente, a interacção entre utilizadores através de textos, publicação de imagens, chat, serviços de mensagens instantâneas, e-mail, vídeo, voz, partilha de ficheiros, blogs, grupos de discussão, etc.

Sugestões para manter a privacidade e Segurança

- Utilize salas com moderador sempre que possível. Estas salas oferecem algum nível de protecção, pois são monitorizadas por moderadores on-line (estes são responsáveis pela triagem das mensagens, eliminando aquelas que consideram inadequadas). O comportamento nestas salas é melhor que em salas não moderadas;
- Antes de iniciar, verifique os termos e condições, o código de conduta e a declaração de privacidade no site do chat;
- Nunca indique onde vive, a sua idade, o seu nome. Não deverá, utilizar algo que o identifique como seja uma alcunha, ou algo que se assemelha com a sua identidade real; a escola que frequenta, o seu telefone, o seu local a de trabalho, ou algo que identifique a sua família. Eduque e vigie os seus filhos no que respeita a actividades nestes ambientes on-line. Por muito simpático que alguém “do outro lado” possa parecer, lembre-se sempre que, na realidade, não faz ideia de quem essa pessoa é;
- Não envie fotografias pessoais para pessoas que conhece em salas de chat;
- Nunca combine encontros, ao fazê-lo, está a correr um risco para a sua segurança pessoal. Em quase todas as circunstâncias, não é boa ideia conhecer alguém em pessoalmente. Se, apesar disto, o fizer, tenha o máximo de precaução. Combine o encontro num local público e faça-se acompanhar de alguém;
- Roubo de identidade e crimes de fraude. Diariamente, ladrões de identidade percorrem salas de chat na Internet procurando pessoas de quem se possam aproveitar. Existem casos de roubo de identidade cujo contacto inicial foi feito através de chat na Internet;
- Não são apenas ladrões de identidade que navegam pelas salas de chat. Sabe-se que todo o tipo de predadores inicia contacto com as suas vítimas através deste meio. Lembre-se que a pessoa pode não ser aquilo que lhe fez crer on-line;
- No caso das crianças é importante que lhe transmita os cuidados a ter. Sugere-se, que o computador se encontre num local comum da casa, e não no quarto da criança. Assim, será mais fácil certificar-se

do tipo de comunicação que é estabelecida e com quem;

Consequências da utilização de Redes Sociais

Os conteúdos de uma Rede Social podem ser armazenados ao longo do tempo por outras entidades (s) terceira (s) que não a Rede Social. Os dados que foram sendo anexados e eliminados ao longo do tempo num determinado perfil, assim como as ligações que foram sendo criadas (ou removidas) ao longo do tempo entre os utilizadores.

Ao longo do tempo os utilizadores podem revelar informações pessoais que poderão ser usadas em contextos que o utilizador não considerou ao revelar essas informações

A informação recolhida pode ser utilizada à posteriori num contexto diferente podendo tornar-se prejudicial para o utilizador. Existem exemplos de empresas que rejeitaram trabalhadores em entrevistas depois de consultarem os respectivos perfis nas Redes Sociais

A informação armazenada numa Rede Social pode ser mudada ou apagada pelo utilizador, no entanto quando estas informações são agregadas por outra (s) entidade (s) não é possível remover essas informações.

Dificuldades na eliminação completa de um perfil

Um utilizador que pretenda eliminar o seu perfil numa Rede Social, verificará que apesar de ser fácil eliminar a página do seu perfil, não conseguirá, em grande parte dos casos eliminar os dados secundários como os comentários e mensagens enviadas aos outros utilizadores

Perigos das redes sociais

Técnicas mais usadas pelos spammers:

- Uso de software especializado que automaticamente envia pedidos de amizade e comentários com publicidade. Estas ferramentas utilizam ainda a pesquisa para que a publicidade que enviam seja a mais dirigida possível;
- Envio de comentários com links (hiperligações) para endereços que pretendem vender um produto.;
- Envio de pedidos de amizade através de perfis que seduzem o utilizador a aceitar esse pedido. Esse perfil contém depois links para sites comerciais ou sites de phishing;
- Envio de comentários para perfis de amigos recorrendo por exemplo à técnica descrita no ponto anterior. As ferramentas de spam angariam o máximo de amigos possíveis, enviando depois o máximo de mensagens para esses amigos;
- Usurpação de passwords de um determinado perfil para a utilização deste no envio de spam;

Infiltrações em círculos de confiança

- Muitas Redes Sociais permitem que informações mais sensíveis, ou todas, estejam disponíveis apenas para os utilizadores dentro do círculo de amizades. Este mecanismo dá, no entanto, uma falsa ideia de protecção aos utilizadores, já que é muito fácil alguém entrar para esse círculo sobre falsos pretextos;
- É possível em algumas Redes Sociais a utilização de scripts ou software especializado como o Friendbot ou o FriendBlasterPro para fazer convites de amizade automáticos e em grande escala;
- A pressão existente nas Redes Sociais e em alguns círculos para a angariação do maior número de amigos leva a que, muitas vezes, se aceitem utilizadores como “amigos” sem conferir a autenticidade do seu perfil;

Esta vulnerabilidade não apresenta uma ameaça directa para os utilizadores, pode no entanto abrir portas a outras vulnerabilidades, permitindo, a um utilizador malicioso ter acesso:

- O visionamento de informações pessoais;
- Procurar informações ou contactos utilizados mais tarde em “ataques”;
- Envio de Spam e acções de marketing.

CyberBullying

O bullying consiste numa perseguição constante de crianças mais velhas ou fortes a crianças mais novas ou fracas, resumindo-se a uma perseguição constante a um (ou vários) elemento mais fracos de um grupo. O CyberBullying consiste no desenvolvimento destas actividades recorrendo às ferramentas disponíveis na Internet.

Neste campo, as Redes Sociais fornecem algumas ferramentas aos perseguidores uma vez que lhes dão meios para concretizarem, as suas acções:

- Facilidade de ataque através de comentários pouco abonatórios e constantes no perfil do alvo;
- Revelação de segredos ou imagens embaraçosas On-line;
- Exclusão premeditada de alguém de um grupo;
- Ameaças físicas;
- Facilidade em manter o anonimato, criando, um perfil falso;
- Facilidade em divulgar os comentários num grupo específico e restrito (Ex: escola);
- As Redes Sociais fornecem todas as ferramentas geralmente utilizadas nestes ataques num único interface: Mensagens Instantâneas, SMS, perfis falsos e caluniosos, difusão controlada de mensagens caluniosas;
- As Redes Sociais não são muito frequentadas por adultos e educadores, o que faz com que estes não se apercebam destas acções.

Recomendações

- **Limite a quantidade de informações pessoais que coloca online**

Não publique informações que o tornem vulnerável (Ex: morada, horários, determinadas situações embaraçosas etc...). Tenha cuidado com as informações que terceiros colocam sobre si On-line;

- **A Internet é um “local” público**

Publique apenas informação que pode ser acessível a qualquer pessoa. Esta recomendação é válida não só para as Redes Sociais como para blogues e outros fóruns de discussão. A partir do momento que coloca informação online não é garantido que esta possa ser completamente removida; por isso tenha extremo cuidado antes de a disponibilizar;

➤ **Esteja atento aos estranhos**

Nunca revele informações importantes a pessoas que não conhece;

➤ **Seja céptico**

Não acredite em tudo que lê on-line;

➤ **Consulte as políticas de privacidade**

Algumas Redes Sociais partilham e vendem as informações dos seus utilizadores a outras entidades;

7) Guia de Utilização de Internet, endereços de alguns sites onde se pode descarregar programas para filtrar e ou limpar informação não desejada

Enuff pc www.enuffpc.com

O objectivo principal do enuff pc é a limitação de tempo de navegação, podendo, decidir que programas podem ou não ser utilizados.

<http://www.microsoft.com> Windows live family Safety

serviço gratuito que ajuda as famílias a ter segurança on-line.

Anti-vírus com Firewall virtual ex. Panda (software não gratuito)

Proteção fácil de utilizar. Basta instalá-lo e e criar uma barreira contra os vírus, spywares e fraudes on-line, compartilhar fotos e vídeos com amigos ou simplesmente navegar na Web, sem preocupações. Pode utilizar a Internet, transferir ou partilhar arquivos que está protegido contra todos os tipos de vírus, worms e Trojans.

<http://free.avg.com/br-pt/download-avg-anti-virus-free>

Navegue e faça pesquisas com segurança.

<http://avast.com.pt> (software gratuito)

Anti-vírus para evitar ataques através do correio electrónico, mensagens instantâneas, aplicações P2P, jogos . Protege dum modo eficaz a informação pessoal, de programas (spyware). Detecta ameaças ocultas em scripts de ficheiros executáveis.

<http://sourceforge.net>

software gratuito

Deep Freeze (software não gratuito)

Programa de recuperação do sistema, aumenta as capacidades e restaura o Windows, tornando-o uma ferramenta de segurança, controle e manutenção do computador. O computador é "limpo" cada vez que se reinicia o sistema operacional, restaura as configurações originais. Exigindo apenas o reinício do computador

<http://weblocker.fameleads.com/getweblocker.asp>

O We-Blocker mantém uma lista de sítios bloqueados. O programa pede autorização para fazer uma actualização automática dessa lista, via Internet, com base numa lista existente e baseada em informações prestadas por outros utilizadores.

O utilizador pode impedir o acesso a sites que contenham palavras ou frases que considera inadequadas. O We-Blocker dá aos pais a oportunidade de monitorizar o acesso à Internet, pois mantém a lista dos sites que foram acedidos. É gratuito.

<http://www.cyberpatrol.com>

O Cyber Patrol carrega durante o arranque do computador e corre em Background para controlar o acesso a todas as aplicações associadas, podendo bloquear o acesso a sites impróprios, gerir o tempo de acesso, controlar a transferência de ficheiros fóruns impróprio ou filtrar mensagens de e-mail, protege a identidade pessoal.

Anti-Porn - <http://www.tueagles.com/anti-porn/>

Filtro anti- pornografia

Censor cop - <http://www.censorcop.com>

Filtra acessos à Internet e bloqueia *software*.

ContentProtect - <http://www.contentwatch.com>

Software que protege de conteúdos impróprios

Cybersitter.99 - <http://www.cybersitter.com>

Este programa limita o acesso de duas formas distintas: bloqueamento e alerta, quando se tenta aceder as áreas seleccionadas.

CyberOptimizer - <http://cyberoptimizer.com>

Um programa que optimiza ligações e bloqueia *sites* inadequados

8) Guia de Utilização de Internet, ferramentas que podem ajudar os pais a obstruírem o acesso de informação não desejada e podem ser agrupados pelas seguintes características:

- ***Ferramentas de limitação de tempo***

Limitam o tempo gasto na Internet, ou evita o acesso nos horários em que os pais não podem supervisionar.

- ***Filtros baseados em listas de sítios***

Restringem o acesso a sítios considerados impróprios.

- ***Filtros baseados em palavras proibidas***

Usam uma lista de palavras encontradas em sítios impróprios e analisam o contexto em que as mesmas se encontram.

- ***Filtros baseados em rótulos de classificação***

Há organizações que classificam e rotulam um local (web ratings systems) usando um sistema conhecido como "PICS" (Platform for Internet Content Selection).

- ***Ferramentas para Bloqueio no envio de dados***

Programas que impedem o envio de dados pessoais pela Internet como o nome, endereço e número do cartão de crédito.

- ***Browsers (navegadores) para crianças***

Programas que auxiliam a criança a aprender usar a Internet, direccionando-as para centros educacionais ou entretenimento na Web.

- ***Motores de busca (pesquisa) para crianças***

São ferramentas de pesquisa existentes na Internet, que podem ser utilizados para pesquisa de assuntos interessantes e adequados, filtrando locais e palavras ou procurando apenas a informação em sítios numa lista seleccionada.

- ***Ferramentas de monitorização***

Estas ferramentas estão escondidas, registando tudo que foi acedido na web (sítios visitados, mensagens de correio recebidas ou enviadas, sessões de conversa, etc.). Se instaladas secretamente, podem provocar ressentimento nas crianças mais velhas por se sentirem espiadas. Estas ferramentas devem ser usadas cuidadosamente pelos pais.

- **Outras opções de segurança**

Alguns programas oferecem outras protecções adicionais como: bloqueio de publicidade, protecção anti-vírus, anti-spam, impossibilidade de acesso ao computador (*firewall*) etc.

9) Guia de Utilização de Internet, sites onde se encontra informações úteis sobre segurança de crianças e jovens na Internet

- www.miudossegurosna.net
- Be Web Aware <http://bewebaware.ca/english/default.aspx>
- ChildNet International <http://www.childnet-int.org/default.aspx>
- CISA - Consumers for Internet Safety Awareness (The Safer Internet Programme)
<http://www.saferinternet.org/>
- Critical Educational Approach to Internet Risk <http://www.safer-internet.net/>
- Portal da Família <http://www.portaldafamilia.org/artigos/artigo051.shtml>
- Promoting Positive and Safe Internet Use <http://www.wisekids.org.uk/index.htm>
- Safer Internet <http://www.safer-internet.net/>
- SAFT <http://www.saftonline.org/>
- Specialists Schools Trust <http://www.schoolsnetwork.org.uk/>
- Seguranet - www.seguranet.min-edu.pt
- Wilders.org security advisors - www.wilders.org

Glossário de termos informáticos úteis

- **Browser**

É um programa ou conjunto de programas que localiza e mostra páginas na Web. Os mais utilizados são: Internet Explorer, Netscape e Mozilla.
- **Chat-Room (Sala de Conversa)**

Local em que duas ou mais pessoas trocam mensagens, em tempo real, através da Internet.
- **Cookie**

Pequena mensagem informativa dada pelo computador servidor ao computador que acede. O browser armazena essa mensagem sob a forma de texto que será transmitida de novo ao servidor todas as vezes que aceder a uma página lá armazenada.
- **Download**

Transferência de ficheiros entre um computador onde estão armazenados e outro computador que os solicita.
- **E-mail (Correio Electrónico)**

Envio e recepção de mensagens entre computadores. As mensagens ficam armazenadas num computador designado por "servidor" ao qual o utilizador se liga para ler ou receber/enviar a mensagem
- **Filtros**

Programas que impedem a entrada de determinados conteúdos ou correio electrónico não desejado.
- **Firewall**

Barramento de acesso do exterior ao computador que está ligado à Web.
- **Fóruns**

Locais abertos de debate ou de informações que versam determinados temas, expostas a leitura para intervenções posteriores ao longo do tempo. Também podem ser designados por *newsgroups* ou conferências.
- **Internet**

Rede mundial de computadores que permite a sua intercomunicação através das várias opções de comunicação actualmente existentes (Ex. Linhas telefónicas de cobre, Fibra óptica, Cabo, ADSL, etc)
- **Mensageiros (Instant Messenger)**

Programas interactivos com potencialidades várias que também permitem mensagens instantâneas, conversas e conferências em tempo real (chat). Alguns têm capacidade de transmissão de imagem e som. Ex.º *MSN Messenger, ICQ, AOL, Mensageiro Sapo, Skype, etc*
- **News (Newsgroups)**

O mesmo que Fóruns
- **Online**

Em tempo real. Os utilizadores de computadores estão *online* quando ligados a outros computadores através da Internet.

- **Phishing (“Pescar” informações dos utilizadores)**

Método de engenharia social quando um desconhecido se faz passar por alguém de confiança, ou por uma entidade, com vista à obtenção de informações que permitam o acesso não autorizado a computadores, informações ou contas bancárias.

Ex: algumas frases às quais deve ter atenção numa mensagem de correio electrónico (não responder Verifique a sua conta”; “Se não responder dentro de 48 horas, a sua conta será fechada

- **P2P (*Peer to Peer*)**

Tipos de programas que permitem ligação entre computadores estando cada um ao serviço dos outros. São muito utilizados para *downloads* de músicas, filmes, software, imagens, ex. *Emule*, etc.

- **Sítio (*Site*)**

Local, na Internet, onde é apresentada informação que pode ser acedida por outros computadores.

As informações podem conter texto e/ou imagens e sons.

- **Spam**

“*Spam*” é o equivalente a correspondência não desejada ou a telefonemas abusivos. Refere-se a todas as mensagens de correio electrónico não solicitadas, que são enviadas para um grande número de indivíduos ou organizações que não consentiram a sua recepção.

- **Spyware**

Programas “espiões” utilizados para obterem informações, sem conhecimento dos utilizadores, dos computadores que estão ligados à Internet. Por exemplo: informações confidenciais - senhas [passwords], id. de cartões de crédito, cookies, etc.

- **URL**

(*Uniform Resource Locator*), em português (Localizador -*Padrão de Recursos*), é o endereço de um recurso (um arquivo, uma impressora etc.), disponível numa rede: Internet e intranet.

- **Vírus**

Programas de informática produzidos para alterarem o funcionamento de outros programas. Os vírus são transmitidos por troca de suportes de armazenamento de informação (CD-ROM's, PEN's, CD's, etc) ou, através da Internet – *e-mails* ou *downloads* e mensagens de telemóvel.

Exemplo de Vírus:

Trojans (Cavalos de Tróia)

É um programa pode vir anexado a num e-mail ou disponível em sites na Internet. Normalmente é recebido como um " presente"(exemplo: cartão virtual de aniversário, álbum de fotos, jogos, etc), para além de executar funções para as quais foi aparentemente projectado, também executa funções normalmente maliciosas e sem o conhecimento do utilizador É necessário que o cavalo de Tróia seja executado para que se instale no computador

Funções que podem ser executadas por um cavalo de Tróia:

Instalação de programas para possibilitar que um hacker tenha controlo total sobre um computador.

- O acesso e a cópia de todos os arquivos armazenados no computador;
 - Descobre todas as senhas utilizadas, e outras informações sensíveis, como sejam os números de cartões de crédito;
 - O controle total sobre o computador;
 - A alteração ou destruição de todos os arquivos.
- **Worms:** têm a mesma finalidade do vírus, mas propagam-se automaticamente, replicando-se assim em grande volume o computador reinicia sozinho e depois não funciona normalmente
- **World Wide Web (WWW)** – Termo utilizado para designar a grande “teia” ou rede que interliga a rede mundial de computadores.