

Segurança na NET



Agrupamento de Escolas
de Vieira de Leiria

Biblioteca/Centro Recursos



Conselhos práticos para crianças

Não cliques em links: Quando conversas por instant messaging ou recebes um e-mail, nunca cliques directamente em quaisquer links. Se a mensagem ou e-mail vierem directamente de alguém que conheces, então escreve o endereço no browser. Se não conheceres a pessoa que enviou, o melhor é ignorá-la.

Não transfiras ficheiros de fontes duvidosas: Certamente recebes com frequência mensagens instantâneas convidando-te a descarregar uma fotografia, uma música ou um vídeo. Por vezes, este ficheiro pode não ter sido enviado pela pessoa cujo nome aparece como remetente, mas sim por um programa malicioso que infectou o teu computador e que se está a distribuir para outros utilizadores. Como salvaguarda, o melhor a fazer é perguntares ao teu contacto se realmente te enviou algo. Caso não o tenha enviado, informa-o que possivelmente foi infectado para que possa eliminar o ficheiro e alertar os seus contactos.

Não fales com estranhos: Em chatrooms ou em instant messaging, nunca podes saber com certeza com quem estás a falar. Especialmente em comunidades online, onde algumas pessoas nunca se encontraram na vida real. Nunca deves criar amizades com estranhos, e em nenhuma circunstância deves encontrar-te com eles na vida real.

Não forneças informação confidencial pela Internet: Nunca envies informação privada (os teus dados, a tua morada, etc.) por e-mail ou instant messaging, e nunca publiques este tipo de informação em blogs ou fóruns. Deves também ter cuidado quando crias perfis para serviços como o Facebook ou Myspace. Nunca deves incluir informação confidencial como a tua idade ou morada. É aconselhável não utilizares o teu nome verdadeiro, mas sim um nome falso ou um pseudónimo.

Fica atento a qualquer suspeita: Se um programa que não te recordas de ter instalado começar a mostrar falsas infecções ou pop-ups a convidar-te para comprar um produto, tem cuidado. Podes ter algum tipo de malware instalado no teu computador.

Não executes ficheiros suspeitos: Se a tua solução de segurança te informar que um ficheiro pode conter ou contém malware, não o abras. Apaga-o apenas.

Fala com os teus pais ou professores: Se tens alguma questão acerca disto, se encontrares algo suspeito ou receberes e-mails ofensivos ou perigosos, fala com um adulto. Eles serão capazes de te aconselhar.



Conselhos práticos para pais

Fale com os seus filhos: O primeiro passo para proteger os seus filhos é falar com eles. Deverá conhecer as páginas que visitam, com quem falam, o que gostam de ver, etc. Não os deixaria sair de casa sem saber para onde vão e com quem vão, logo, não deverá deixá-los aceder à Internet sem saber o que estão a fazer.

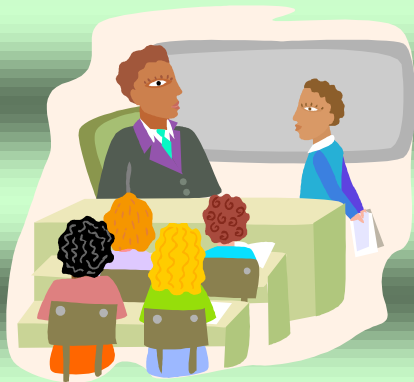
Aprenda por si, e passe o conhecimento para os seus filhos: Para muitos pais a Internet ainda é um mundo desconhecido. Alguns utilizam-na para procurar informação, ler o jornal ou transferir músicas, files e outros ficheiros, mas muitos outros, os serviços e as páginas que os seus filhos utilizam são completamente desconhecidos. Como tal é muito importante conhecer as ferramentas que a Internet oferece às crianças, e quais os riscos que existem e como evitá-los. Quando obtiver estes conhecimentos já pode aconselhar os seus filhos sobre como utilizarem a Internet de forma segura.

Defina regras firmes para a utilização da Internet: Deve estabelecer regras claras e firmes, controlando o tempo máximo online e a forma como utilizam a Internet. Certifique-se que cumprem as regras, especialmente no que diz respeito à utilização da Web de noite. Outro aspecto a considerar é a localização dos computadores em casa: se possui apenas um PC para toda a família, deve encontrar-se numa divisão familiar e não no quarto da criança.

Proíba as crianças de fornecerem informação confidencial: Deve instruir os seus filhos para não fornecerem dados como o nome, morada e fotografias pela Internet. Aconselhe-os a utilizar nomes falsos ou pseudónimos em fóruns e mostre-lhes como criar palavras-passe seguras (misturando letras maiúsculas com minúsculas) para impedir que ciber-criminosos ou outros utilizadores maliciosos acedam às suas contas de e-mail ou messaging.

Ensine os seus filhos a estarem atentos às aparências: As aparências também iludem na Internet. Já verificámos códigos maliciosos disfarçados de codecs ou trailers de filmes; as formas como os pedófilos se fazem passar por outras pessoas para estabelecer contacto com crianças, ou a forma como mensagens que parecem provir de um contacto conhecido podem estar infectadas. Logo, na Web as coisas nem sempre são o que parecem. Ensine os seus filhos a estarem alerta e para não fazerem nada que possa colocar em causa a sua segurança ou privacidade.

Instale uma solução de segurança eficaz: Para proteger os seus filhos de códigos maliciosos, a melhor estratégia é possuir uma solução de segurança eficaz e actualizada. A Panda oferece soluções para utilizadores domésticos que não se limitam a eliminar malware, bloqueando também páginas Web que possam infectar os computadores, filtrando spam e, no caso do Internet Security, inclui uma funcionalidade de controlo parental que lhe permite seleccionar que páginas os seus filhos poderão aceder.



Conselhos práticos para professores

Os professores têm um papel importante no fornecimento da informação sobre as formas correctas de utilizar as novas tecnologias, a crianças e jovens acima de tudo, já que os computadores são actualmente comuns nas salas de aula. É por isso que fornecemos uma série de recomendações a seguir:

Descubra: Procure e leia informação acerca das ameaças da Internet. Descubra o que são e quais as suas consequências, e como pode transmitir esta informação aos jovens.

Desenvolva um plano de educação relacionado com segurança das TI: Tal como os jovens aprendem a lidar com computadores e com a Internet, devem também aprender sobre os potenciais perigos. Desta forma, garantirá que se mantêm seguros desde o primeiro momento. O melhor procedimento é desenvolver um plano a seguir, preparar o que lhes transmitirá e fornecer a documentação que julgue necessária.

Torne as suas explicações agradáveis e práticas: uma boa forma de ensinar estes conceitos é utilizando exemplos práticos. Pode demonstrar alguns dos perigos da Internet mostrando aos seus alunos alguns dos efeitos que podem causar. Descubra novas histórias relacionadas com casos reais.

Ensine-os a proteger-se: Durante aulas práticas, mostre aos jovens como configurar um antivírus e criar palavras-passe seguras, e explique como comprar online de forma segura, etc

Para mais informações:

<http://www.seguranet.pt/index.php?section=2>