GUIA PARA A SEGURANÇA NA INTERNET

internet segura.pt

PARE

LEIA com atenção

AVANCE com segurança

Julho 2007

ÍNDICE

SOBRE O PROJECTO INTERNET SEGURA

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

A par de todas as possibilidades e benefícios da utilização das TIC, nomeadamente no acesso ao conhecimento e no relacionamento com outras pessoas e organizações, é necessário criar mecanismos e estratégias de minimização de eventuais abusos e ilegalidades possibilitados pela utilização destas tecnologias. No Plano Nacional para a Sociedade da Informação "LigarPortugal", adoptado pelo Governo em Julho de 2005, refere-se a necessidade de "garantir que todos, e em particular as famílias, dispõem de instrumentos para protecção de riscos que possam ocorrer no uso da Internet".

Com o objectivo de fornecer generalizadamente informação sobre uma utilização segura da Internet e de dotar os cidadãos de um canal para comunicação de conteúdos ilegais ou lesivos foi criado o projecto Internet Segura da responsabilidade de um consórcio entre a UMIC – Agência para a Sociedade do Conhecimento (entidade coordenadora), a Direcção Geral de Inovação e Desenvolvimento Curricular/CRIE, do Ministério da Educação, a Fundação para a Computação Científica Nacional – FCCN e a Microsoft Portugal. Este projecto foi submetido ao programa europeu *"Safer Internet Plus"* da Comissão Europeia, tendo sido aprovado.

O Guia para a Segurança na Internet é um contributo do Consórcio para que qualquer utilizador possa, de forma simples, ter informação sobre uma utilização segura e consciente da Internet.

Julho 2007

A IMPORTÂNCIA DA INTERNET

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

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

"Mas, tal como na vida real, também na Internet são necessárias precauções no desenvolvimento de actividades. Já imaginou o que pode acontecer, caso não tome as devidas precauções?"

Pode disponibilizar os códigos de acesso e os números de cartões de crédito a estranhos. Como? Por exemplo, respondendo a uma mensagem de correio electrónico que lhe solicita o envio de palavras passe, nomes de início de sessão, números de bilhete de identidade, ou outras informações pessoais.

Pode possibilitar a utilização da sua conta de acesso à Internet por quem não autorizado. Como? Por exemplo, quando consulta um *site* que pede dados da conta de acesso à Internet, sendo este um *site* forjado.

Pode permitir que estranhos acedam, alterem ou destruam dados pessoais ou institucionais sob a sua responsabilidade. Como? Por exemplo, pela instalação de um programa de forma dissimulada, sem o seu conhecimento.

Pode encontrar informação que nem sempre é verdadeira ou conteúdos que são ilegais. Como? Por exemplo, através do acesso a informação em *sites* pouco fidedignos ou que incitem à violência.

OS PRINCIPAIS DESAFIOS NA UTILIZAÇÃO DA INTERNET

Milhões de utilizadores em todo o mundo navegam na Internet diariamente e, apesar de na maior parte dos casos nada de prejudicial aconteça, a rede mundial não está livre de ameaças.

PARE

O facto da Internet possuir características particulares (facilita a reprodução, alteração e transmissão de conteúdos, não possui "fronteiras", está sempre ligada, entre outras) obriga os utilizadores a adoptarem um conjunto de comportamentos de segurança.

LEIA

Ao navegar na Internet, leia atentamente todas as mensagens com avisos de sistema que possam surgir. Alguns poderão dar origem à instalação de programas concebidos para roubar informação do sistema e enviá-la para terceiros mal intencionados ou, até mesmo, apenas para danificar o seu computador. Consulte o Glossário para conhecer algumas destas ameaças.

AVANCE com Segurança

Para aumentar a segurança do seu computador pessoal, basta seguir alguns conselhos simples e básicos, que protegem o computador de muitos dos problemas identificados.

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

As mensagens instantâneas e outras formas de conversação *on-line* são ferramentas úteis e divertidas utilizadas, não apenas para pura diversão, mas também para efeitos de trabalho.

PARE

Como qualquer meio de comunicação *on-line* tem os seus riscos, a utilização consciente de tais meios de comunicação é a melhor forma de prevenção dos utilizadores, ao permitir acautelar e prevenir fraudes, utilizações abusivas ou outras formas de aproveitamento ilícito por parte de terceiros.

LEIA

Roubo de identidade, crimes de fraude, vírus e cavalos de Tróia são perigos comuns em salas de conversação ou através da utilização de sistemas de mensagens instantâneas. Pode acontecer que estranhos tentem ganhar a confiança dos utilizadores para que estes aceitem mais facilmente ficheiros lesivos ao seu computador.

É também cada vez mais frequente, ser nas redes sociais virtuais que se inicia o contacto com desconhecidos que poderão tentar roubar dinheiro, identidade ou até mesmo provocar danos físicos ou emocionais. Mesmo uma alcunha poderá ser suficiente para o identificar, pelo que deverá evitar essa utilização.

Um pouco como na vida real, os encarregados de educação deverão educar os seus filhos a respeitar estes princípios de segurança também em ambiente virtual.

AVANCE com Segurança

Não use o seu nome verdadeiro. Não deverá usar o seu nome verdadeiro como identificador de entrada em qualquer sala de conversação ou aplicação de mensagens instantâneas. Mesmo uma alcunha poderá ser suficiente para o identificar.

Nunca divulgue informação pessoal. Não deverá revelar onde vive, que idade tem, o seu nome verdadeiro, escola ou local de trabalho, ou qualquer outra informação que o identifique a si ou à sua família.

Nunca combine encontros com estranhos. Mas se combinar, o utilizador deverá garantir que vai acompanhado com alguém responsável e que mais pessoas estão informadas sobre o seu paradeiro.

Não aceite ficheiros enviados por quem não conhece. É muito comum os sistemas informáticos serem infectados com vírus, cavalos de Tróia ou *spywares* enviados por correio electrónico ou directamente através da aplicação de conversação *on-line*. Mesmo de utilizadores que conhece, garanta que tem um antivírus instalado e analise cuidadosamente tudo o que lhe for enviado.

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

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

PARE

A utilização massiva do correio electrónico tornou este meio de comunicação mais vulnerável ao seu uso com objectivos maliciosos. Por esta razão, é fundamental adoptar um conjunto de comportamentos de segurança.

LEIA

Alguns dos problemas podem ser receber mensagens que:

- São indesejáveis;
- Exponham o utilizador a conteúdos indesejados e maliciosos;
- Infectem o computador com vírus, *spywares* e *worms;*
- Conduzam o utilizador a esquemas de fraude *on-line*.

AVANCE com Segurança

Suspeite de qualquer mensagem de correio electrónico de origem desconhecida, mesmo que o seu conteúdo pareça inofensivo à primeira vista.

Não clique em *links* que possam eventualmente aparecer no conteúdo da mensagem de correio electrónico. É aconselhável copiar o *link* e colá-lo no seu navegador de Internet.

Desconfie sempre dos ficheiros enviados em anexo, mesmo os enviados por quem conhece. O endereço do remetente poderá ter sido forjado (esquema habitualmente utilizado por intrusos e conhecido por *spoofing*).

Utilize uma aplicação de antivírus actualizada para verificar os ficheiros em anexo de uma mensagem de correio electrónico. Só se devem abrir ficheiros ou executar programas em anexo, após confirmar que não trazem consigo vírus ou programas maliciosos.

Verifique a veracidade das mensagens com informação alarmante, consultando outras fontes. Não divulgue ou reencaminhe mensagens fraudulentas ou falsas (também conhecidas por *hoaxes*).

Utilize mensagens de correio electrónico cifradas caso necessite enviar informação confidencial. Existem várias soluções comerciais e gratuitas que cifram mensagens enviadas de um sistema para outro ou que limitam o acesso a utilizadores previamente identificados.

As crianças e jovens olham para a Internet como um mundo fascinante que utilizam não só como ferramenta de aprendizagem, mas também para lazer e divertimento.

PARE

Onde está localizado o computador em sua casa e o acesso à Internet? Já conversou com os seus filhos sobre as regras de segurança que devem ter em conta quando navegam na Internet? Já navegou com os seus filhos na Internet? Conhece os sítios por onde eles costumam navegar? Já conversou com eles sobre a lista de contactos que cada um tem nos programas de comunicação em directo pela Internet?
É importante que os seus filhos naveguem de forma crítica, esclarecida e segura na Internet!

LEIA

Converse com os seus filhos e construam em conjunto regras de utilização da Internet com que todos concordem e que sejam razoáveis (local mais adequado, horários e tempo de utilização). Informe-se e contribua para a educação dos seus filhos:

- existe na Internet um conjunto enorme de recursos de qualidade que pode ajudar a melhorar as aprendizagens dos seus filhos;
- a propriedade intelectual e os direitos de autor dos textos, das imagens e dos vídeos que se encontrem *on-line* têm de ser respeitados e obrigam a que sejam sempre referidas as suas fontes quando utilizados noutras situações;
- os jogos *on-line* têm muitas vezes sistemas de mensagens instantâneas incluídos e promovem a presença prolongada dos mais jovens em frente ao computador;
- atenção aos muitos serviços pagos existentes na Internet;
- tenha em atenção a possibilidade de os seus filhos terem nas suas listas de contactos pessoas desconhecidas;
- os conteúdos na Internet devem ser lidos de forma crítica e, em muitos casos, devem ser confrontados com informações provenientes de outras fontes.

AVANCE com Segurança

Actualmente a Internet é uma ferramenta fundamental na progressão das aprendizagens das crianças e dos jovens, mas estes deverão ser alertados para os cuidados a ter durante a sua utilização. Explique aos seus filhos que:

- não devem falar com desconhecidos na Internet, tal como não o fazem normalmente no dia-a-dia;
- devem proteger informação confidencial, não devem expor a sua vida privada na Internet nem divulgar informações sobre a sua família;
- devem validar a informação que retiram da Internet com a existente em outras fontes;
- devem reconhecer a ilegalidade da pirataria, nomeadamente de jogos, música, filmes e aplicações de *software*;
- devem acautelar-se para os perigos dos vírus e de outras aplicações prejudiciais ao computador.

"A *Linha Alerta* é um serviço que pretende possibilitar denúncias de conteúdos ilegais na Internet.
O seu objectivo é agilizar e tornar mais eficaz o tratamento destes casos."

A Linha Alerta visa, nomeadamente, conteúdos do tipo:

- Pornografia infantil;
- Apologia do racismo e xenofobia;
- Apologia do terrorismo e violência.

Tais conteúdos poderão estar alojados em páginas *web*, *e-mail* ou *newsgroups*. Em qualquer dos casos, o anonimato será sempre garantido à pessoa que faça a denúncia.

Para comunicar um conteúdo ilegal ou lesivo visite o *site* **http://linhaalerta.internetsegura.pt**.

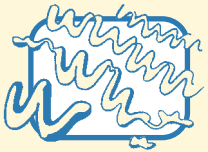
***Phishing* ("Pescar" informações dos utilizadores):** método de engenharia social através do qual um desconhecido se faz passar por alguém de confiança, ou por uma entidade, com vista à obtenção de informações que permitam o acesso não autorizado a computadores, informações ou contas bancárias.
Ex: algumas frases às quais deve ter atenção numa mensagem de correio electrónico: "Verifique a sua conta."; "Se não responder dentro de 48 horas, a sua conta será fechada."

Vírus: na sua maioria encontram-se incluídos no código de programas ou ficheiros e poderão danificar o seu computador ao propagar-se de ficheiro em ficheiro e até mesmo de computador em computador.
Ex: o computador tem um funcionamento mais lento do que é habitual.

Exemplo de Vírus:

***Trojans* (Cavalos de Tróia):** geralmente camuflados num programa legítimo, executam outras funções com o desconhecimento do proprietário do equipamento.
Ex: o sistema apresenta mensagens de erro pouco usuais.

Outro exemplo de Vírus:



Worms: têm a mesma finalidade do vírus, mas propagam-se automaticamente, replicando-se assim em grande volume.
Ex: o computador reinicia sozinho e depois não funciona normalmente.

Spyware: é um "*software*" malicioso que permite a recolha de informação do computador do utilizador por parte de desconhecidos. Na generalidade, o *spyware* poderá vir integrado em programas não fidedignos, ou em determinadas componentes transferidas, quando se acede a um *site* de Internet.
Ex: existem várias formas de o *spyware* ou outro *software* indesejado entrar no seu computador. Um truque comum é instalar o *software* sub-repticiamente durante a instalação de um outro *software* de que necessita, como um programa de partilha de ficheiros de música ou de vídeo.

***SPAM*:** é o conceito utilizado para mensagens de correio electrónico não solicitadas, enchendo as caixas de correio dos utilizadores e aumentando o volume de tráfego na rede.
Ex: mensagens publicitárias de correio electrónico.

1. Quando faz compras *online,* como pode ajudar a manter seguras as informações do seu cartão de crédito?

A. Utilizar palavras passe seguras.

B. Comprar apenas em lojas que apresentem o ícone de cadeado de *site* seguro.

C. Evitar comprar em computadores partilhados e/ou públicos.

D. Todas as anteriores.

2. Se receber uma mensagem de correio electrónico que parece ser *spam*, o que deve fazer?

A. Responder ao emissor da mensagem.

B. Apagá-la sem a abrir, nem clicar nas ligações que ela possa conter.

C. Clicar na mensagem para ver quem a enviou e poder denunciá-lo.

D. Encaminhá-la para um amigo, para pedir a sua opinião.

3. Para ajudar a impedir que as suas crianças vejam correio electrónico ofensivo, qual das seguintes acções é importante?

A. Dar aos seus filhos os seus próprios endereços de correio electrónico assim que saibam utilizar um rato.

B. Abrir todos os anexos no correio electrónico dos seus filhos, mesmo se não souber de quem é a mensagem de correio electrónico.

C. Utilizar filtros de correio electrónico para ajudar a bloquear *spam*.

D. Proibir a utilização de correio electrónico a crianças entre os 2 e os 12 anos de idade.

Veja as respostas certas em **www.internetsegura.pt**

Códigos de acesso ou *Passwords*

- ☑ Códigos de acesso distintos para os diferentes serviços (banca *on-line*, correio electrónico, entre outros...).
- ☑ Não são utilizados nomes, datas relevantes ou dados pessoais.
- ☑ Os códigos de acesso têm mais de 7 caracteres, utilizando maiúsculas e minúsculas, números e/ou outros símbolos.
- ☑ Os códigos de acesso são alterados periodicamente.
- ☑ Os códigos de acesso não se encontram guardados no computador ou noutros locais de acesso fácil.

Segurança do computador

- ☑ O sistema operativo e demais programas encontram-se actualizados.
- ☑ O antivírus está instalado e actualizado.
- ☑ A *firewall* está instalada e a funcionar correctamente.
- ☑ Na utilização de serviços garantir a segurança da ligação (https://).
- ☑ Os principais ficheiros e documentos têm cópia de segurança.

Correio Electrónico

- ☑ O remetente da mensagem é conhecido e a informação não é duvidosa.
- ☑ Verificar a existência de vírus ou aplicações prejudiciais ao computador antes de abrir ou executar os ficheiros.
- ☑ Os *links* constantes da mensagem devem ser copiados e colados no navegador de Internet.

SIMPLES REGRAS DE SEGURANÇA

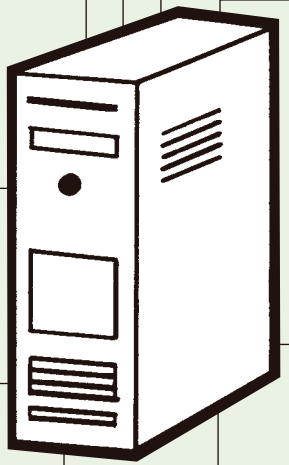
Manter o sistema operativo e aplicações de *software* actualizados

Possuir uma *firewall* instalada no computador

Possuir uma aplicação antivírus instalada e actualizada

Efectuar cópias de segurança regularmente

Escolher códigos de acesso fortes e seguros, bem como e alterá-los periodicamente



Não divulgar ou enviar por meios electrónicos os códigos de acesso a ninguém

Não guardar códigos de acesso no computador ou noutro local acessível por terceiros

Não abrir mensagens de correio electrónico de origem desconhecida. Deve certificar-se previamente quanto à autenticidade das mensagens e ter em especial linha de conta os anexos das mensagens

Ao efectuar transacções na Internet deverá certificar-se que está perante uma ligação segura (https://)

www.internetsegura.pt

Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

Microsoft
O seu potencial. A nossa paixão.

Ministério da Educação

UMIC
Agência para a Sociedade do Conhecimento
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

Co-financiado pela União Europeia
Safer Internet *plus*

LigarPortugal