nova aprendizagem
AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

ama

Guia @prender

Segurança na Internet

número 8

A utilização da Internet **tem claramente vários riscos associados**, mas as **vantagens** relacionadas com a sua utilização superam em muito esses **riscos**. Contudo, estes devem ser conhecidos e minimizados ou mesmo anulados, caso seja possível.

Qualquer equipamento que tenha acesso às funcionalidades da Internet é susceptível de sofrer "ataques" externos, alguns sem intenção danosa, mas muitos com intenções maliciosas. Os serviços de correio electrónico, blogues, redes sociais, fóruns e chats são ferramentas potencialmente vulneráveis a ataques vários, sejam de vírus informáticos ou tentativas de acesso a dados pessoais.

As situações de risco mais comuns são:

Spam

São mensagens de correio electrónico não solicitadas, normalmente associadas a publicidade, e que são muito susceptíveis de se associar a situações de *phishing*. Os emails para listas ou as cadeias de solidariedade são formas de angariar novos endereços onde se vai poder difundir uma actividade maliciosa. Como precaução deve verificar sempre a origem deste tipo de mensagens e a sua credibilidade.

Vírus

Um vírus é um programa que tem como propósito criar um mau funcionamento num dispositivo, muitas vezes corrompendo o seu sistema operativo. Nas situações mais gravosas, executam funções com o desconhecimento do proprietário e permitem o acesso remoto aos nossos computadores.

Phishing

Método suportado no correio electrónico através do qual um indivíduo se faz passar por alguém conhecido ou por uma entidade com o objectivo de se apropriar de informação que permita o acesso não autorizado a sistemas, informações e a contas bancárias. Como exemplo, os casos em que se criam páginas falsas de entidades bancárias e, no processo de entrada nas contas, se solicita a actualização de dados online, como códigos de acesso ou números de contribuinte. As instituições fidedignas não procedem desta forma para actualização de dados. O propósito deste acto fraudulento é aceder a informação pessoal que permita aos burlões aceder à sua identidade e debitar contas ou cometer crimes em seu nome.

Cyberbullying

O cyberbullying pode ser definido como um conjunto de ameaças e intimidações feitas via Internet (via sites, blogs), redes sociais (twitter, facebook ou outros), instant messaging (msn, skype), etc., por um indivíduo ou um grupo, com a intenção de prejudicar outrem. Com a utilização massificada das redes sociais este é um fenómeno em crescimento que afecta, principalmente, crianças e jovens em idade escolar.

Para nos protegermos dos riscos na Internet podemos adoptar dois tipos de atitudes. A protecção técnica e a protecção assumida através da utilização de comportamentos seguros...

A segurança da internet pode ser feita pelo lado da tecnologia, das redes informáticas e hardwares associados e pelo lado da segurança pessoal, relacionada com o acesso de cada um dos utilizadores. A primeira é um caso de concepção, desenho e manutenção das redes e equipamentos informáticos, planeamento de antivírus, firewall, etc. A segunda tem a ver com o posicionamento e atitude dos utilizadores face ao mundo que a Internet nos oferece.

Atitudes de carácter técnico	Atitudes comportamentais
Utilize uma firewall. Desta forma estará a impedir o acesso ao seu computador por parte de estranhos, através da Internet. Ligar-se à Internet sem uma firewall é como deixar a porta de casa aberta.	**Nunca divulgue informação pessoal**. Não revele qualquer tipo de informação que o identifique a si ou à sua família, onde vive, nem o local de trabalho.
Actualize o computador. Garantir que o sistema operativo e programas instalados apresentam as últimas actualizações é um importante reforço de segurança.	**Não combine encontros com estranhos**. Se tiver de o fazer, garanta que vai acompanhado e que informa diversas pessoas de confiança sobre o seu paradeiro.
Configure o seu navegador de Internet para bloquear pop-ups. Em sites da Internet pouco fidedignos pode acontecer que os pop-ups transportem código malicioso de informações enganadoras ou de endereços manipulados.	**Não aceite ficheiros de quem não conhece**. Estes ficheiros podem conter vírus. Mesmo de utilizadores que conhece, garanta que tem um antivírus instalado e analise cuidadosamente tudo o que lhe for enviado.
Instale antivírus e antispyware. É importante que o computador tenha estes programas instalados e actualizados de modo a precaver-se contra ameaças externas.	**Suspeite** de qualquer mensagem de correio electrónico de remetente desconhecido, mesmo que o seu conteúdo pareça inofensivo à primeira vista.
Certifique-se que os sites que visita são fidedignos. Nos sites fidedignos esteja atento para situações fora do normal ou pedidos de informação pessoal, evitando cair em esquemas de phishing. Nunca siga os endereços que lhe são enviados por correio electrónico, mensagens instantâneas ou em pop-ups.	**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.
	Verifique a veracidade das mensagens com informação alarmante, de cadeias de solidariedade e desconfie sempre que lhe quiserem oferecer qualquer tipo de prémio só por estar online.

Devemos ter uma atitude permanente de segurança face à internet e à sua utilização!

Não Esquecer!

Estarmos protegidos no "mundo virtual" pode ser trabalhoso mas é fundamental para evitarmos transtornos maiores. A maioria dos esquemas e fraudes pode ser evitada se estivermos atentos e praticarmos uma "navegação" responsável!

nova-aprendizagem@ama.pt
http://www.rcc.gov.pt/novaaprendizagem