**Cuidados a ter enquanto navega na web**

Autor: CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática

Os ataques informáticos a que estamos sujeitos têm evoluído e, neste momento, o seu computador pode ficar infectado com um vírus simplesmente por visitar um site, mesmo que legítimo. A partir desse momento pode ter um vírus no seu computador que permite ao atacante fazer o que quiser, incluindo roubar todas as suas *passwords*.

Para diminuir a probabilidade de ser infectado existem algumas medidas que pode tomar. Primeiro que tudo não deve usar uma conta com acesso de administrador para navegar na web. A maioria dos computadores vem com o Windows configurado de forma a que o utilizador tenha total controlo do computador. Isto faz com que um vírus que consiga penetrar o seu computador também possa ter total controlo do mesmo.

A melhor forma de proteção é ter as suas aplicações actualizadas. Incluindo um antivírus instalado e com os *updates* em dia. A grande maioria dos ataques são feitos explorando falhas nas aplicações de uso comum tais como o *Acrobat Reader*,o *Flash Player* ou o Java. Se não tiver este software devidamente atualizado, aumentará o número de falhas que podem ser exploradas.

Além dos vírus deverá também ter cuidado com as suas *passwords*. Não utilize a mesma *password* em diversos sites. Se não conseguir lembrar-se de todas as *passwords*, use uma aplicação para gestão de *passwords*, que usa uma chave-mestra para proteger as outras. A *password* do seu email deve, no entanto, ser diferente de todas as outras, visto que o acesso ao seu email permite a um potencial atacante aceder a muitas outras *passwords* (utilizando o mecanismo de recuperação de *passwords*).

Também deve evitar fazer *login* em contas importantes a partir de redes *Wi-Fi* públicas ou abertas. Um atacante pode facilmente obter acesso a todas as comunicações que faça nas mesmas e pode, inclusivamente, fazê-lo pensar que está a fazer login na sua conta de *email* quando na verdade está a fazer *login* numa página criada pelo atacante para roubar a sua *password*. Neste caso verifique sempre se está a ligar-se via HTTPS e não HTTP. Se o endereço a que está a aceder começar por http:// não está em modo seguro, se for https:// está.

---------------------------------------------------------------------------

**Mês Europeu da Cibersegurança**

Este artigo é da autoria de especialistas do CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática (www.cert.pt) da FCCN-Fundação de Computação Científica Nacional (www.fccn.pt/pt) e insere-se na campanha "Uma dica por dia" integrada no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013.

O Mês Europeu da Cibersegurança é uma iniciativa da ENISA - Agência Europeia para a Segurança das Redes e Informação (www.enisa.europa.eu) e o seu objectivo é informar os utilizadores sobre a importância da segurança da informação, bem como demonstrar algumas medidas simples para proteger os seus dados.

------------------------------------------------------------------------------

**Nota aos editores da Imprensa regional**

Os artigos da autoria dos técnicos do CERT.PT incluídos no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013, surgem no site da Ciência na Imprensa Regional numerados, de forma a permitir a sua mais fácil identificação. No entanto, eles são absolutamente independentes uns dos outros e podem ser publicados pelos órgãos de comunicação de forma avulsa.

------------------------------------------------------------------------------

Foto de Bojanaz

(Existem ficheiros de imagem de alta resolução disponíveis para download)