**Correio eletrónico: cuidados a ter**

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

Já ninguém passa sem o uso do correio eletrónico (*email*). Facilidade de utilização, velocidade de transmissão, facilidade de integração e fornecimento de contas gratuitas, fazem o seu sucesso. Este não escapa, porém, a tentativas menos bem intencionadas por parte de alguns internautas. Existem, no entanto, algumas boas práticas para o seu uso que melhoram a sua segurança.

Evite a utilização da sua conta de *email* empresarial para uso pessoal. Crie uma ou até mais contas pessoais num dos serviços gratuitos para o efeito tal como o *gmail* ou *Yahoo.* Sugerimos a criação de duas, uma para tratamento de assuntos pessoais ou para registos em *sites* importantes, outra para registo em *sites* de menor relevância. Além de permitir maior privacidade, garantirá alguma salvaguarda na divulgação das suas contas mais restritas, protegendo-se dos *spammers*.

Escolha uma palavra-passe (*password*) forte e distinta para cada conta. Evite como *password* datas, nome dos filhos ou do cão, (*passwords* fáceis de deduzir). Use letras minúsculas e maiúsculas, números e carateres especiais na sua criação e um mínimo de 8 carateres.

Caso o seu antivírus o permita, configure-o para efetuar a análise ao e*mail* em *tempo real*.

Não permita que o seu cliente de *email* guarde a sua *password*, sobretudo no caso do dispositivo de acesso ser partilhado por mais pessoas.

Nunca abra anexos que provenham de remetentes desconhecidos salvaguardando-se assim de possíveis vírus. Caso receba alguma mensagem com anexo de um seu conhecido mas cujo conteúdo lhe pareça suspeito (uma mensagem em inglês de alguém que lhe escreve sempre em português, por exemplo), antes de abrir valide com o remetente se a mensagem é fidedigna.

Desconfie de mensagens com *links* no seu interior, nunca clique sobre algum sem antes passar o cursor do rato sobre ele verificando no canto inferior esquerdo do seu *browser* se o *link* corresponde de facto ao site a que deve corresponder (faça-o cuidadosamente e tenha em atenção que um endereço do tipo www.empresa.xpto.com NÃO pertence à EMPRESA mas sim ao site da entidade XPTO). Nunca responda a mensagens de SPAM, nem clique em *links* do seu conteúdo. Ao fazê-lo, está a confirmar que o seu *email* é valido.

Caso lhe sejam solicitados dados pessoais ou credenciais de acesso, valide sempre com o remetente, por outra via, se a mensagem enviada é verdadeira. E evite enviar *passwords* por *email*, use antes o telefone.

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

**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.

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

Ilustração de Alexander Bedrin

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

