**Identificar uma mensagem de correio eletrónico fraudulenta**

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

Sendo o correio eletrónico (*email*) dos serviços mais usados na Internet, este é também dos serviços mais usados por internautas com intuitos ilegais. O objetivo destes é aceder à sua informação pessoal, a passwords ou levá-lo a clicar em determinados *links* para poder vir a obter essa informação.

Não sendo Portugal um dos alvos preferidos das redes internacionais que se dedicam a estas actividades, acontece que muitas das mensagens que servem de veículo a estes intuitos estão longe de ser perfeitas. O comum é encontrar uma mensagem cujo texto está escrito em mau português, contendo erros ortográficos, gramaticais, frases pouco coerentes ou termos brasileiros.

Por este tipo de fraude ter um tempo de vida curto, é normal ser-lhe solicitado que seja rápido na resposta ao *mail* ou que seja rápido em clicar num *link*.

Mesmo que a mensagem tenha um aspeto verosímil, deve olhar atentamente para o remetente, para validar a autenticidade da mensagem. Se não reconhece o remetente, se não parecer formar qualquer palavra/nome, ou se o remetente e a mensagem não parecerem ter qualquer relação, não responda. Se se tratar de uma mensagemrelacionada com uma situação interna da sua organização, verifique se reconhece o *email* e, caso tenha dúvidas, valide-o com o seu administrador de sistemas.

Se lhe solicitarem que clique num *link*, por mais autêntica que a mensagem lhe possa parecer, nunca o faça sem antes passar com o rato sobre o *link* verificando de seguida no canto inferior esquerdo do seu *browser* para que endereço vai ser reencaminhado. Caso o domínio do *link* seja externo ao domínio da sua organização, reencaminhando-o para uma página fora desse domínio, não clique. Valide o *link* através do site <https://www.virustotal.com/pt/#url> ou através de um contato do representante da suposta entidade remetente do email ou com o seu administrador de sistemas.

Os bancos nunca tratam de assuntos privados dos seus clientes por *email* por isso, caso receba uma suposta mensagem da sua entidade bancária, contate-a telefonicamente quanto antes.

As mensagens mais comuns deste tipo consistem em comunicar-lhe que é finalista de um concurso que o pode tornar milionáro, que existe um problema com a sua conta de *email*, que é necessário validar urgentemente os seus dados bancários, etc.

Qualquer técnica é boa para tentar usurpar-lhe dados pessoais. Seja céptico.

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

**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 Selim Aksan

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

