

IDENTIFIQUE E-MAILS FALSOS

Dicas fundamentais para conseguir identificar mensagens fraudulentas, provenientes de pessoas que pretendem a todo o custo apoderar-se indevidamente dos seus dados mais importantes e até do seu dinheiro.

SAIBA COMO:

- Reagir a más intenções de pessoas sem escrúpulos
- Proteger os seus dados pessoais e a sua conta bancária
- Detectar a tempo e horas armadilhas de que seja alvo

Na antiguidade, os ladrões tinham cara de maus, usavam uma arma e eram violentos. Hoje em dia, a versão digital e moderna desses criminosos mudou radicalmente de perfil. Actualmente, os ladrões modernos valem-se da tecnologia e do anonimato para roubar dados e até mesmo dinheiro sem que, muitas vezes, a vítima se aperceba dessas maldades. Por norma, esse roubo ocorre a partir de uma simples mensagem de *e-mail*. Pode parecer absurdo, mas o número de fraudes *online* tem crescido de forma assustadora. Apesar de Portugal ter um número de casos bastante pequeno quando comparado com os Estados Unidos, por exemplo, é importante conhecer alguns truques simples e eficientes para ninguém ser apanhado de surpresa. Nada é mais prudente do que conhecer a forma de acção dos bandidos digitais para não ter a desagradável surpresa de ver dados pessoais roubados ou a conta bancária deixada a zero da noite para o dia.

U m a forma bastante comum de acção e de propagação de *e-mails* falsos chama-se *phishing*. Através desta prática maliciosa, os ladrões virtuais usam abor-

dagens que parecem ser de empresas com as quais a maioria de nós, normalmente, realiza transacções comerciais, como administradoras de cartão de crédito, bancos, lojas *online* e até mesmo instituições de caridade. Visualmente, estas mensagens parecem-se com autênticos comunicados oficiais, mas, o principal objectivo não é outro senão obter dados pessoais ou outras informações importantíssimas, como *passwords* de acesso a contas bancárias. No fundo, o que os ladrões virtuais pretendem com o *phishing* é literalmente pescar dados no seu computador. Para lograr esses intentos maliciosos, a maior parte dos ataques por *phishing* tenta induzir o utilizador a digitar informações importantes, como dados da conta bancária, *passwords* de acesso, núme-

