

## Evite a fraude: Como pode proteger-se

A UNICEF está muito preocupada com o uso fraudulento do nosso nome e do nosso logo por indivíduos sem escrúpulos que abusam deliberadamente da confiança que a UNICEF merece por parte dos seus apoiantes em todo o mundo. Em seguida apresentamos detalhes sobre o modo como a fraude tem sido cometida – e como ajudar a proteger quer a UNICEF quer a si próprio de consequências potencialmente graves.

### Ofertas fraudulentas

Temos recebido relatos de que alguns impostores poderão estar a utilizar o nome e a credibilidade da UNICEF para aliciar o público através de sítios da Web, e-mails e telefonemas. Estes abusos estão a ser estudados pelo departamento jurídico da UNICEF em Nova Iorque. A UNICEF e os seus Comités Nacionais estão a alertar o público no sentido de evitar que se abuse da boa vontade dos nossos apoiantes para obter dados pessoais.

Assim, alertamos para o facto de alguns sítios da web, e-mails e telefonemas que oferecem emprego ou prémios em nome da UNICEF são inventados e fraudulentos. Só a UNICEF e os seus 36 Comités Nacionais estão autorizados a enviar comunicações ou apelos dirigidos ao público em nome da UNICEF.

### Atenção ao ‘phishing’

Dado o aumento da atenção que os media têm dedicado ao roubo de dados pessoais, muitos consumidores – bem como apoiantes de organizações humanitárias como a UNICEF – estão preocupados com a privacidade e integridade dos seus dados pessoais.

Por esse motivo é importante estar a par da existência da correspondência fraudulenta via Internet, também conhecida como ‘phishing’.

‘Phishing’ é um tipo de fraude na qual as mensagens por e-mail, mensagens instantâneas e sítios Web são usados para convencer os utilizadores a fornecer informações pessoais e confidenciais. O termo remete para a ideia de que as pessoas irão ‘morder o isco’ e fornecer informações pessoais, que podem ser usadas para cometer fraudes com cartões de crédito e outras violações graves da privacidade.

Os e-mails ‘phishing’ parecem ser geralmente enviados por organizações legítimas, pedindo aos utilizadores que respondam ou cliquem num link para uma página web a fim de actualizar a sua informação pessoal. Por vezes contêm o logo da organização e até uma direcção postal, mas o endereço web, ou URL, não coincide com o da organização legítima.

### Não se deixe ‘apanhar’

Alguns dos dados habitualmente solicitados pelos ‘phishers’ são o nome e endereço do utilizador; número de Segurança Social; números de contas bancárias e palavras-chaves e informação relativa a cartões de crédito — por vezes até o nome de solteira da mãe do titular ou outra informação privada usada por questões de segurança.

Eis algumas medidas que pode tomar para evitar ser ‘apanhado’ por um esquema de ‘phishing’: Fique alerta face a um e-mail inesperado, uma mensagem instantânea, mensagem de voz ou fax que pretenda ser proveniente de um banco, empresa de cartões de crédito, serviço on-line ou organização de solidariedade com a qual tenha uma conta ou da qual seja membro;

No caso de receber uma mensagem dessa natureza, ligue para o número de apoio ao cliente ou para a organização (e não para qualquer número indicado na mensagem) para confirmar se é legítima;

Não responda a instruções de qualquer e-mail, telefonema ou fax que o convidem a divulgar as suas informações pessoais;

Não faça clic em quaisquer links incluídos no e-mail suspeito; fazer clic num link desses pode levar ao download de programas de key-logging ou 'spyware' para o seu computador;

Aceda regularmente ao seu *online banking*, cartões de crédito e outras, e verifique os seus extractos de conta para se assegurar que todas as transacções são legítimas;

Utilize software anti-vírus actualizado – incluindo filtros spam e até programas 'anti-phishing', que estão disponíveis para ajudar a barrar potenciais 'phishers' em sítios web e e-mails.

### Exemplos de fraude



O [screenshot](#) acima mostra como o nome da UNICEF pode ser usado abusivamente para fins fraudulentos on-line. A conferência anunciada não está de modo algum ligada ao trabalho legítimo da UNICEF. De facto, este apelo é um exemplo de uma falsa conferência internacional – uma variante do bem conhecido 'Nigerian 419', esquema de pagamento antecipado/lotaria falsa, no qual as pessoas são ludibriadas para fazer transferências de dinheiro através da Internet.

Por favor não responda a quaisquer comunicações que o incitem a responder para um endereço que não pertence à UNICEF.

Uma outra mensagem com o título "Global Opportunity from UNICEF" tem circulado como um apelo de recolha de fundos. A mensagem pede dados confidenciais e oferece uma comissão às pessoas que aceitarem donativos em nome da UNICEF. A mensagem "Global Opportunity" é fraudulenta, a UNICEF não actua nem se associa a qualquer esquema de fundraising semelhante. O falso endereço UNICEF de retorno é uma conta de Gmail.

### Exemplos de E-mails Fraudulentos (Portugal)

Através dos nossos doadores, clientes e amigos tivemos conhecimento deste e-mail que nos deixou bastante incomodados, pois nada tem a ver com a UNICEF.

Não responda a este tipo de e-mails que o incitem a divulgar esta mensagem pelos seus contactos.

Lamentamos o abuso por parte de pessoas sem escrúpulos que se servem de imagens terríveis de crianças e usam indevidamente o nome da UNICEF para fins que desconhecemos.

