



# Correio Eletrónico





## INTRODUÇÃO

O correio eletrónico, mais conhecido por e-mail, é o meio de comunicação mais utilizado no ciberespaço. Atualmente, torna-se fundamental termos em conta alguns fatores úteis para proteger as nossas contas de e-mail.

Muitas fraudes que provêm de atacantes, não são facilmente identificáveis, pelo que podem existir falhas de segurança que expõem os dados pessoais dos utilizadores. Nada garante que um endereço de e-mail permaneça seguro sem que existam algumas precauções. Por exemplo, alguns fatores tais como, a configuração de palavras-passe fortes, a alteração das mesmas com frequência, a utilização de serviços de e-mail que recorram a autenticação (tendo em conta os filtros de spam, instalação de antivírus e anti-spam, baseados em desktop).

É de referir que, um fornecedor de serviços garante a segurança de e-mail, através de palavras-passe fortes e mecanismos de controlo de acesso a um servidor de e-mail.

## ANEXOS DE EMAIL

Ao abrir anexos para destinatários que não se conhece, é necessário ter algum cuidado. Um anexo descarregado pode ser, ou até conter, um software malicioso proveniente de uma fonte não fidedigna. Verifique sempre o formato de documento que recebe no e-mail e seja prudente com os ficheiros executáveis, que possam permanecer no seu computador ou dispositivo móvel.

## ENGENHARIA SOCIAL

Verifique se o remetente da mensagem recebida é confiável. No caso de se tratar de um remetente desconhecido, não abra o e-mail, não clique nas ligações, nem aceite os anexos.

Não clique em links que promovam propaganda ou publicidade enganosa, pois pode colocar o seu computador em risco, através da instalação de *malware*.

## ASSINATURA DO EMAIL

Quando falamos em assinatura de e-mail, é necessário ter alguns cuidados com as informações que se divulgam aos destinatários. Quando se trata de e-mails profissionais, deve-se considerar as políticas definidas pela entidade profissional.

## ENVIAR EM BCC

Em caso de partilha de um e-mail para muitos endereços de correio eletrónico, pode enviar através do campo Bcc ou Cco. Esta funcionalidade faz com que quem recebe o e-mail apenas visualize o remetente, não causando incómodo, em caso de não partilha do e-mail com terceiros.

## EXEMPLOS DE EMAILS FALSIFICADOS

Caro(a) Cliente,

Em anexo enviamos-lhe a sua Fatura Electrónica edpID nº 287001223522 emitida em 2012-09-24 relativa ao local de consumo C223-9082.

A sua fatura está também disponível para consulta na sua área de cliente [edpOnline](#), acessível em [www.edp.pt](#). Poderá ainda consultar o seu histórico de consumos, comunicar leituras e gerir alterações contratuais.

Disponibilizamos nos anexos os esclarecimentos adicionais que consideramos necessários através do nº 808 53 53 53, todos os dias úteis das 9h às 20h. Poderá ainda contactar-nos por e-mail em [edpcliente@edp.pt](mailto:edpcliente@edp.pt) ou visitar-nos no site [www.edp.pt](#).

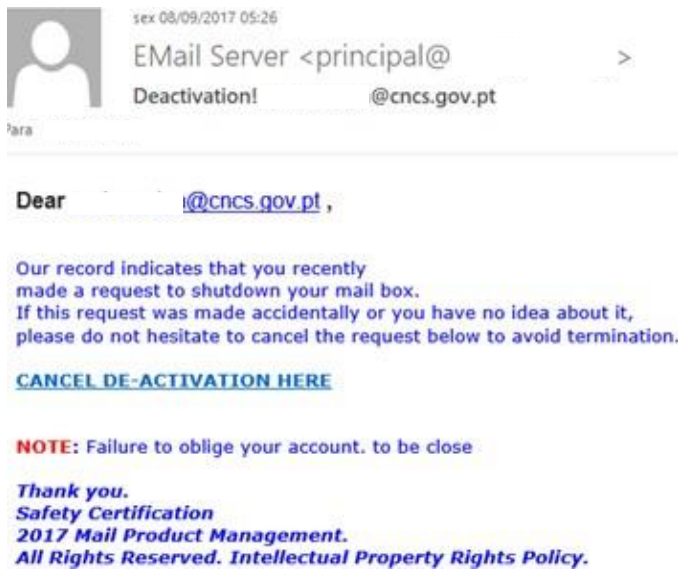
Com os melhores cumprimentos,

Serviço ao Cliente  
EDP Comercial

[287001223522.pdf \(389 KB\)](#)

### ATAQUE DE PHISHING

Sob a visualização de uma suposta fatura eletrónica, os destinatários deste e-mail falsificado, em nome de uma entidade, são induzidos a aceder a ligações que remetem para páginas fraudulentas na Internet. O utilizador incorre no risco de infetar o seu computador com software malicioso que permite a terceiros aceder ao computador para fins ilícitos, como a recolha de dados e a recolha de informação confidencial para uso fraudulento.



### ATAQUE DE PHISHING

Através da receção de um email falsificado para o endereço eletrónico da pessoa, induz ao acesso a um link fraudulento para o cancelamento da ativação de um serviço, visando infetar o computador com software malicioso.

To:  
Subject: Mensagens e alertas: 1 nova mensagem!  
From: [bfa.net@bfa.ao](mailto:bfa.net@bfa.ao)  
Date: Mon, 14 Dec 2015 12:56:11 +0100



Prezado BFA Cliente,

Você recebeu uma mensagem não lida na sua conta BFA Online Banking sua chave de confirmação é diferente da sua senha login certifique-se de digitar a chave de confirmação corretamente para key sua conta atualizada.  
[VER SUA MENSAGEM](#)  
Banco BFA ©2015. All rights reserved.Terms and conditions

### ATAQUE DE PHISHING

Um ataque pode ser realizado através de e-mails falsificados que contêm uma ligação fraudulenta que é passível de comprometer a privacidade e segurança do cliente ao pedir a sua palavra-chave do Online Banking

De: Emailbox [<mailto:georgiadou@ipcd.gr>]  
Enviada: 5 de setembro de 2017 02:46  
Para: | [@cncs.gov.pt](mailto:@cncs.gov.pt)  
Assunto: Email UPDATE

Dear,

Your email account ([@cncs.gov.pt](mailto:@cncs.gov.pt)) quota is full  
This may cause your email account so Impaired or you may no longer receive more emails.

To continue using your email account, you Require immediate upgrade to your mailbox with increased quota.  
This service is free.

[Upgrade Mailbox Quota Here](#)

Once the upgrade is complete, your email account will work effectively.

Mail Service 2017.

### ATAQUE DE PHISHING

Este exemplo de fraude ocorre com o pedido de realização de uma atualização fraudulenta, o cancelamento da ativação de um serviço em que o utilizador não é cliente. As ações de clicar em ligações pode comprometer os seus dados pessoais e profissionais.

# Proteja-se para ser ciberseguro/a.



*O presente conteúdo é propriedade do Centro Nacional de Cibersegurança estando protegido nos termos da legislação de propriedade intelectual aplicável. O utilizador pode copiar, importar ou usar gratuitamente parte ou a totalidade da informação, para uso pessoal ou público, desde que não tenha finalidades lucrativas ou ofensivas e seja referida a fonte de informação.*