

Diário Leiria

04-12-2018

Periodicidade: Diário

Classe: Informação Geral

Âmbito: Regional

Tiragem: 2008

Temática: Economia

Dimensão: 489 cm<sup>2</sup>

Imagem: N/Cor

Página (s): 8

## Defesa do Consumidor

DECO

## Como evitar fraudes no homebanking

A internet facilita a gestão da conta bancária, os investimentos e as compras online, mas pode apresentar riscos que devemos evitar.

Ter homebanking é uma das formas mais cómodas de obter informações sobre produtos e serviços do banco, realizar operações bancárias, fazer pagamentos, entre outras operações, sem sair de casa. No entanto, existem dois tipos de fraude informática que deve saber distinguir,

mas mais importante ainda, saber como evitar.

O phishing é um método usado para aceder a dados confidenciais, como o nome de utilizador, palavra-chave do cartão bancário e outros elementos pessoais que, posteriormente, serão vendidos a terceiros ou utilizados para fazer operações sobre contas existentes ou para abertura de novas contas bancárias. O ataque informático, por norma, é feito via e-mail, simulando uma mensagem comum do banco.

O pharming, também identificado como um tipo de fraude, recorre a uma técnica mais complexa que o anterior. Neste caso, pretende-se que o endereço de um site remeta para um servidor diferente do desejado, levando o utilizador a fornecer os seus dados pessoais, convicto que a página é fidedigna. Estes dados, tal como no phishing, são depois utilizados para transferências fraudulentas. Se usa regularmente o homebanking aconselhamos que adote alguns comportamentos para evitar as burlas:

- Altere com frequência a palavra-chave;

- Atualize regularmente o antivírus e o anti-spyware do computador;

- Não aceda ao site do banco através de links enviados em e-mails ou em mensagens. Evite também fazê-lo recorrendo aos favoritos, histórico ou recorrendo aos resultados apresentados em motores de busca. Deve digitar sempre o endereço na barra do browser;

- Não abra anexos de mensagens não solicitadas, mesmo que pareçam enviadas por conhecidos;

- Não envie o seu nome de utilizador, código de acesso ou cartão-matriz por e-mail;

- Desconfie de mensagens com endereços estranhos ou português incorreto;

- Nunca insira dados pessoais em páginas que não garantam uma ligação segura, isto é, que não comecem por 'https://';

- Termine sempre a sessão quando aceder ao website do seu banco;

- Consulte periodicamente a sua conta bancária;

- Consulte a lista de instituições autorizadas a prestar serviços bancários no site do Banco de Portugal.

Relativamente aos direitos e deveres do cliente bancário em caso de fraude, informamos que se o consumidor tiver cumprido os deveres de confidencialidade e segurança dos seus dados, ao comunicar a operação não autorizada ao banco, deverá ser reembolsado. O cliente tem um período de 13 meses, a contar desde a data do débito, para comunicar ao banco as operações de pagamento não autorizadas.

Recai sobre o banco o risco das falhas e do deficiente funcionamento, e terá de ser o banco a provar que a operação de pagamento não autorizada nunca teve a ver com avaria técnica ou com outra deficiência do sistema. ◀

Isa Tudela  
Gabinete de Projetos e Iniciativas  
(DECO/Coimbra)  
(artigo escrito com o actual  
acordo ortográfico)