manchete

Jornal Notícias
Suplemento
28-10-2018

Periodicidade: Diário
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 110603
Temática: Tecnologia
Dimensão: 1106 cm²
Imagem: S/Cor
Página (s): 25

SERVIÇOS BANCÁRIOS

O que fazer se for vítima de fraude *online*

Usar o computador ou o *smartphone* para realizar operações bancárias já faz parte do nosso dia-a-dia. Mas, há que ser cauteloso. Se desconfiar que está a ser vítima de fraude deve agir rapidamente.

—SARA FERNANDES
sara.fernandes@dinheirovivo.pt

Fazer pagamentos pela internet é cada vez mais comum. Seja através de *homebanking* ou até mesmo através de aplicações de telemóvel. Hoje em dia, transferir dinheiro é tão fácil e rápido como enviar um simples sms.

A facilidade na realização destas operações tornou-nos também mais vulneráveis a burlas. Há vários tipos de fraude. No mundo digital, destacam-se duas formas: o *phishing* e o *pharming*. O *phishing* é um método usado para conseguir obter dados confidenciais, tais como o nome de utilizador, palavra-chave do cartão bancário e outros elementos pessoais que depois serão vendidos a terceiros ou usados para fazer transações sobre contas existentes ou abertura de novas contas. Nestes casos, o utilizador recebe um *e-mail* de alguém que se faz passar pelo banco. O *pharming* recorre a uma técnica mais complexa. O objetivo é fazer um endereço de um *site* remeter para um servidor diferente do pretendido. Ao ter a aparência de uma página fidedigna, quando solicitado, o utilizador fornece os seus dados pessoais (*login*, números de conta e senhas de acesso, por exemplo), que depois são usados para transferências fraudulentas.

Se desconfiar de que está a ser vítima de fraude deve agir rapidamente. O primeiro passo a dar é contactar o seu banco e pedir o cancelamento das credenciais de acesso ao *homebanking* ou, se for o caso, do cartão. Depois, deve participar a situação à polícia ou ao Ministério Público. Estes são os conselhos do Banco de Portugal.

Direitos e deveres

No caso de alertar o seu banco, não será chamado a pagar quaisquer valores que forem movimentados após esse alerta. Daí a importância de agir rapidamente. Contudo, para os valores que sejam movimentados antes disso, pode ter de suportar até um máximo de 150 euros. Já se não tiver cumprido as regras de segurança, aí terá de pagar valores superiores a 150 euros.

A Deco explica que se o banco não demonstrar que o cliente foi negligente e mesmo que não se saiba como é que terceiros acederam aos dados, o consumidor tem o direito de ser reembolsado. Se isso não acontecer no momento, o cliente tem direito a receber juros de mora.

Cuidados a ter

Existem alguns cuidados extra para evitar burlas. A Deco aconselha a alterar a palavra-chave com alguma regularidade, atualizar o antivírus do computador com frequência, não aceder ao *site* do banco através de *links* enviados por *e-mail*, desconfiar de mensagens com endereços estranhos ou português incorreto, nunca inserir dados pessoais em páginas que não garantam uma ligação segura (ou seja, que não comecem por "https://") e terminar sempre a sessão do portal do seu banco antes de sair. Por via das dúvidas consulte também a lista de instituições autorizadas a prestar serviços bancários no *site* do Banco de Portugal.

E não se esqueça: não faz parte do procedimento dos bancos pedir aos clientes para enviarem os seus dados pessoais, até porque tem apostado em formas de validação cada vez mais sofisticadas nos seus *sites*, para maior segurança dos clientes. Por isso, desconfie sempre se receber *e-mails* com estes pedidos.

Não se esqueça: não faz parte do procedimento dos bancos pedir aos clientes para enviarem os seus dados pessoais por *e-mail*. Desconfie sempre.

MÓNICA MONTEIRO

Dicas
Como proteger a sua conta *online*

—Palavra-chave
É aconselhável que mude a sua palavra-chave com frequência. Altere-a de três em três meses, por exemplo.

—Antivírus
Faça a atualização do antivírus regularmente. Apesar de não haver defesas 100% eficazes, sempre consegue impedir algumas ameaças.

—Aceder ao *site*
Não aceda ao *site* do banco através de *links* enviados em *e-mails* ou a partir de resultados apresentados em motores de busca. O ideal é escrever sempre o endereço na barra do *browser*.

—Dados pessoais
Não envie o seu nome de utilizador, código de acesso ou cartão-matriz por *e-mail*. Nem nunca insira os seus dados pessoais em páginas que não comecem por "https://".

—Lista de instituições
O Banco de Portugal disponibiliza no site uma lista das instituições autorizadas a prestar serviços bancários. Por isso, sempre que tiver dúvidas, faça uma consulta.