manchete

Diário Económico
Finanças Pessoais
16-10-2015

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 18714
Temática: Banca/Seguros
Dimensão: 1774
Imagem: S/Cor
Página (s): 4/5

12

DICAS ANTI-PHISHING

Como evitar que o saldo da conta bancária seja pescado na "rede"

Há cerca de uma semana, diversos portugueses receberam mensagens supostamente de três dos maiores bancos portugueses, onde era solicitada a actualização do cartão matriz das respectivas contas bancárias. Mas estes emails nada mais eram do que um ataque de "phishing". Os ciber-criminosos visavam encaminhar as vítimas desse ataque para um site falso onde lhes era solicitada a introdução de dados pessoais, nomeadamente a palavra-passe, colocando as contas bancárias em risco. Conheça 12 dicas que o poderão ajudar a evitar que a sua conta bancária fique à mercê dos ataques informáticos. **Catarina Melo**

1 **NÃO DIVULGUE DADOS CONFIDENCIAIS** É um alerta que os bancos não se cansam de fazer: nunca solicitam aos clientes a divulgação ou a alteração de dados pessoais e confidenciais através de mensagens de correio electrónico ou por SMS. Por isso, sempre que tal lhe seja solicitado o mais provável é estar a ser alvo de uma tentativa de 'phishing' com o objectivo de capturar os dados do deu cartão matriz ou dos códigos de acesso ao sistema de 'homebanking' para posterior utilização fraudulenta. Por isso, se receber uma mensagem ou contacto nesse sentido, não forneça qualquer informação e elimine a mensagem da caixa de correio electrónico.

2 **CONTACTE O BANCO SE SUSPEITAR DE 'PHISHING'** Sempre que lhe solicitem via mensagem de correio electrónico a divulgação de dados pessoais alerte o seu banco para essa situação. Mas nunca o faça através dos contactos enviados nesse e-mail, mas sim através da linha de apoio telefónico da instituição financeira. Visite também o site do banco já que a maioria das instituições financeiras disponibiliza nas suas plataformas 'online' um leque de informação a alertar para os perigos e a principais medidas de prevenção para fazer face a esse tipo de situações.

3 **SUSPEITE DE 'LINKS' E FICHEIROS** Duvide sempre dos emails em que lhe é pedida qualquer acção ou interacção já que podem conter vírus que se instalam no computador. Não responda, não clique em 'links' nem abra ficheiros de remetentes desconhecidos ou aceda à plataforma de 'homebanking' através de um 'link' recebido por email. Um dos truques mais usados por criminosos para ter acesso a contas bancárias pela internet é a criação de sites falsos de bancos, mas que se assemelham às páginas verdadeiras. Por isso deve verificar sempre o endereço do site (URL) antes de inserir as informações da sua conta. Opte ainda por digitar manualmente na barra de endereços do 'browser' o endereço completo do site a que pretende aceder para evitar cair nessa armadilha.

4 **SOLUÇÃO ANTIVÍRUS EFICAZ** Uma das formas dos ciber-criminosos chegarem aos dados de acesso ao serviço de 'homebanking' é através da instalação de vírus no computador da vítima. Uma forma de prevenir que isso aconteça - apesar de não ser impeditivo já que estão sempre a surgir novos vírus - é possuir uma solução de antivírus de qualidade e que seja constantemente actualizada.

5 **PRESERVE CÓDIGOS** Evite utilizar nomes de clubes de futebol, nomes próprios ou que possam ser de fácil dedução (12345, 111111, data de nascimento, etc) nas 'passwords' de acesso aos sites bancários. Periodicamente, deverá também alterar os seus códigos.

6 **ATENÇÃO À LINGUAGEM** Nos emails fraudulentos é frequente identificar no texto erros de escrita grosseiros ou expressões pouco habituais e que facilmente excluem a possibilidade de se tratar de uma comunicação autêntica do banco. Isto acontece porque a maioria parte dos ataques informáticos têm origem fora de Portugal, em países como a Rússia ou a China, em que muitas vezes são utilizadas traduções automáticas.

7 **SISTEMAS OPERATIVOS ACTUALIZADOS** Uma forma de prevenir que o seu computador seja atacado por ciber-criminosos é manter o sistema operativo sempre actualizado. Utilize também uma "firewall" no seu computador. Trata-se de um programa que lhe possibilita filtrar o tráfego da Internet que entra e sai do seu computador, tornando mais difícil o contágio por malware.

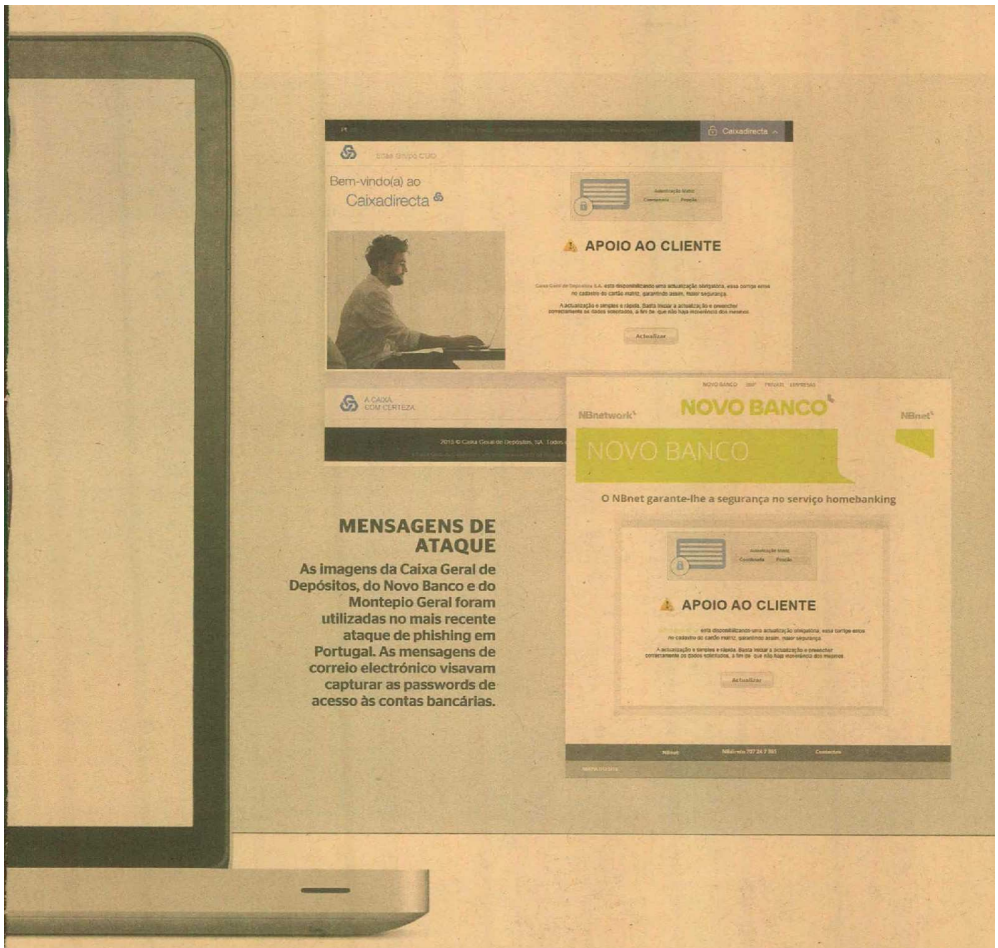
8 **EVITE ACEDER AO SERVIÇO EM COMPUTADORES PÚBLICOS** Nunca deve aceder ao serviço de 'homebanking' a partir de computadores públicos já que estes podem estar contaminados por mecanismos que capturam dados dos dispositivos que a elas acedam. Sempre que possível, entre na sua conta apenas a partir da rede Wi-Fi da sua casa ou de seu plano 3G/4G. Não se esqueça ainda de terminar sempre a sessão através da opção 'sair'. Desta forma, garante o término da sessão, evitando que esta possa ser retomada por outra pessoa.

manchete

Diário Económico
Finanças Pessoais
16-10-2015

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 18714

Temática: Banca/Seguros
Dimensão: 1774
Imagem: S/Cor
Página (s): 4/5



MENSAGENS DE ATAQUE
As imagens da Caixa Geral de Depósitos, do Novo Banco e do Montepio Geral foram utilizadas no mais recente ataque de phishing em Portugal. As mensagens de correio electrónico visavam capturar as passwords de acesso às contas bancárias.

PALAVRA-CHAVE

'Phishing'
Fraude informática na qual o criminoso se faz passar por uma instituição para tentar persuadir (através de um mail) alguém a divulgar informação pessoal. Deste modo, o autor da fraude fica na posse de palavras-passe e números de contas bancárias.

'Malware'
São programas informáticos maliciosos - como vírus ou "cavalos de tróia" - cujo o objectivo é infiltrarem-se no sistema de um computador para causar algum tipo de dano. Em ataques de 'phishing', os 'malware' destinam-se a roubar informações confidenciais da vítima.

9 PROTEJA O 'SMARTPHONE' Apesar da abundância de informação, muitos utilizadores ainda acreditam que vírus, ataques informáticos e outros problemas de segurança ocorrem apenas nos computadores. Na verdade, esquecem-se que os 'smartphones' e 'tablets' passam cada vez mais horas ligados à Internet e, consequentemente, estão também muito expostos a esse tipo de riscos. Por isso, aplique a este tipo de equipamentos os mesmos cuidados de segurança que devem ser tomados nos computadores. Dificulte ainda o acesso indevido ao seu 'smartphone', protegendo-o com uma 'password'. Estes equipamentos podem ser facilmente perdidos ou roubados.

10 EFECTUE NEGÓCIOS APENAS COM EMPRESAS CONHECIDAS E FIDEDIGNAS Antes de concretizar uma compra 'online' certifique-se de que o site onde o pretende fazer tem garantia de segurança. Estas páginas têm o símbolo de um cadeado e o URL tem a seguinte indicação https://, em vez de http://. Contudo, não há nenhuma forma de garantir segurança absoluta. Os sites devem também ter sempre uma declaração de privacidade que indica espécificamente que a empresa não transmitirá o seu nome e informações a outras pessoas.

11 MONITORIZE AS SUAS TRANSACÇÕES Reveja as confirmações das suas encomendas e os extractos dos cartões de crédito e bancários quando os recebe para se certificar de que lhe estão a ser cobradas apenas as operações que efectuou.

12 CRIANÇAS À DISTÂNCIA Estabeleça limites e crie regras de utilização da Internet. Por exemplo, implemente restrições de acesso para impedir os mais novos de instalar ou de executar programas que não sejam do seu conhecimento. Explique ainda aos mais novos que nem tudo deve ser partilhado na internet e nas redes sociais e que a utilização dos computadores/'smartphones' deve ser efectuada de forma responsável.