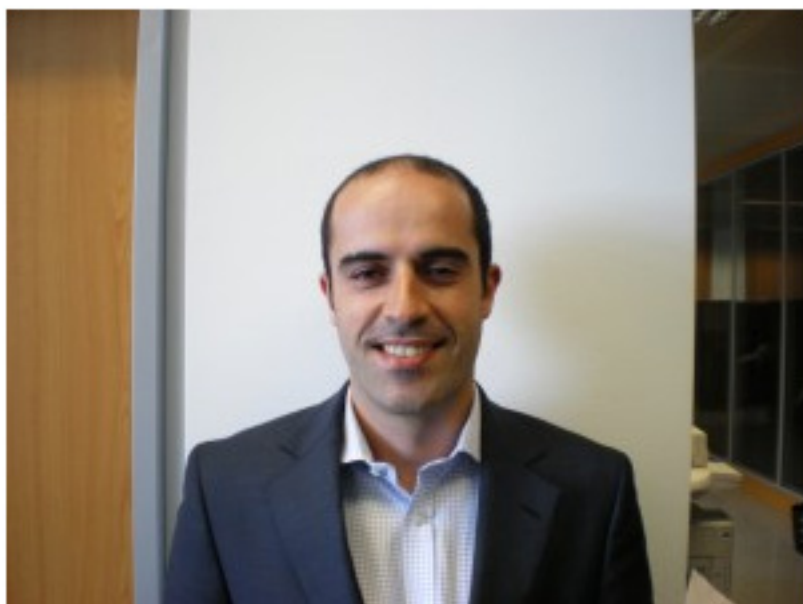


## Como tornar o acesso ao homebanking uma experiência segura?

19 de Novembro de 2010 às 17:30:14 por Pedro Fonseca

Rodrigo Borges  
Consultor de Soluções de Infra-estruturas de Segurança  
CESCE SI



A utilização do homebanking (banca online) tem-se generalizado nos últimos anos. Permite a redução de custos à entidade bancária e agiliza o acesso dos clientes à sua conta e às operações bancárias.

A par do crescimento da utilização do homebanking, têm crescido também as fraudes online e o número de clientes lesados, embora nem sempre estas informações venham a público, nem a grande maioria dos clientes se aperceba no imediato que algo aconteceu. Muitas vezes os bancos assumem os custos de falhas de segurança de modo a não perderem o cliente e manterem a sua boa imagem.

Para combater este crime, existem 3 pilares fundamentais:

- Utilização de um PC seguro.
- Comportamento consciente dos utilizadores.
- Melhoria das funcionalidades das páginas de homebanking.

### Utilização de um PC seguro:

O primeiro passo para garantir um acesso seguro é usar um PC de confiança.

Evite aceder ao homebanking a partir de um PC que não o seu e nunca a partir de um PC público ou partilhado.

Garanta que o PC tem as actualizações (segurança e outras) do sistema operativo instaladas.

Garanta que o PC tem antivírus instalado, actualizado e que faz a limpeza com uma frequência mínima semanal.

Garanta que o PC tem uma aplicação de limpeza de software malicioso instalada, actualizada e que faz a limpeza com uma frequência mínima semanal. Sugere-se o uso da aplicação **CCleaner**. É gratuito e eficaz.

Como medida de protecção adicional sugere-se o uso da aplicação **Trusteer Rapport**. Esta aplicação gratuita isola e protege o acesso a qualquer página (assim o utilizador a indique), evitando que qualquer outro processo intercepte a sessão e capture informação. Esta aplicação faz também uma análise ao PC e sugere um conjunto de acções para aumentar a segurança deste.

Apesar de me referir apenas à utilização de um PC, o acesso ao homebanking via telemóvel ou PDA deverá reger-se pelas mesmas regras de segurança.

### Comportamento consciente dos utilizadores:

É importante que os utilizadores não confiem que o banco lhes dará toda a protecção. Cabe aos utilizadores protegerem-se contra os perigos.

Mesmo que o PC esteja seguro, se os utilizadores não tiverem um comportamento consciente sobre a sua utilização, estarão a facilitar a vida aos criminosos. Assim, os utilizadores devem evitar o acesso a páginas potencialmente perigosas e evitar o uso de aplicações de partilha de ficheiros, entre outros. Se tiverem que o fazer, façam-no a partir de um computador público, ou efectuem uma limpeza cuidadosa do PC após utilização.

Mude de password com frequência mínima trimestral. Sendo que a ideal seria frequência mensal. Se a password for capturada, pode ser que consiga alterá-la antes de ser usada.

Use todos os mecanismos de autenticação adicionais disponibilizados pelo banco: matrizes, sms, ou tokens. Dificulte ao máximo o acesso aos criminosos.

Active todas as possíveis notificações de movimentos na conta, mesmo que por um pequeno preço. Seja notificado de qualquer operação.

Recuse todo e qualquer phishing (mails falsos a solicitar informação sobre a sua password ou matriz). Os bancos nunca lhe enviarão qualquer email, nem lhe pedirão para aceder a qualquer página onde terá que introduzir os seus dados. Se mesmo assim tiver dúvidas, contacte o atendimento a clientes e confirme a veracidade desse pedido antes de o aceitar.

Existem inúmeras dicas para despistar um acesso malicioso, **como as seguintes**:

1 – Minimize a página. Se o teclado virtual for minimizado também, está correcto. Se ele permanecer no ecrã sem minimizar, é pirata! Não teclé nada.

2 – Sempre que entrar no site do banco, digite a sua password errada na primeira vez. Se aparecer uma mensagem de erro significa que o site é realmente do banco, porque o sistema tem como verificar a password digitada. Mas se digitar a password errada e não acusar erro é mau sinal. Sites piratas não têm como conferir a informação, o objectivo é apenas capturar a password.

3 – Sempre que entrar no site do banco, verifique se no rodapé da página aparece o ícone de um cadeado; além disso clique 2 vezes sobre esse ícone; uma pequena janela com informações sobre a autenticidade do site deve aparecer. Em alguns sites piratas, o cadeado pode até aparecer, mas será apenas uma imagem e ao clicar 2 vezes sobre ele, nada irá acontecer.

### Melhoria das funcionalidades das páginas de homebanking:

Os bancos têm a sua quota-parte de responsabilidade na utilização segura do homebanking. Devem garantir um bom serviço, disponibilizar os meios para os utilizadores controlarem a sua conta e implementarem internamente mecanismos de protecção à fraude online.

Informe-se junto do seu banco do que este "oferece" para melhorar o serviço homebanking.

Sugira e exija todas e quaisquer melhorias que considere válidas para a segurança do serviço.

Se o banco desprezar, ou menosprezar, as suas preocupações sobre a segurança do homebanking, então talvez esteja na altura de procurar uma alternativa.

Se não pretender usar o serviço de homebanking, então bloqueie a sua conta errando repetidamente a password.

Se detectar qualquer actividade suspeita na sua conta, recolha o maior número de informação possível, bloqueie imediatamente o acesso à sua conta errando repetidamente a password o número de vezes necessárias, desligue o PC e contacte o seu banco e as autoridades judiciais.

O serviço de homebanking nunca será 100% seguro. Mas é possível diminuir consideravelmente o risco e continuar a beneficiar da sua utilização.