**Utilizar a banca online**

Autor: CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática

Quase todos os bancos nacionais disponibilizam aos seus clientes serviços de banca eletrónica através da Internet, que permitem a realização de operações bancárias comuns, no conforto da sua casa ou no trabalho. Pela sua importância, estes serviços possuem um conjunto de mecanismos de segurança, tais como cartões-matriz e códigos enviados por SMS. Pela mesma razão, são um alvo apetecível. Grupos de criminosos utilizam diversos esquemas a que se dá a designação de *phishing* para conseguir, de uma forma direta ou indireta, elementos de segurança que lhes permitam fazer-se passar por si e apoderar-se dos seus bens.

Para evitar estes esquemas deve ter em atenção que o seu banco NUNCA usa o email para pedir informação, visto que este meio é reconhecido como um canal inseguro. Por este motivo, deve ignorar qualquer email que lhe peça informação ou solicite que aceda a uma determinada página da Internet.

No caso de haver algum problema com o seu cartão-matriz, o banco gera um novo. E em caso algum lhe pede mais que uma pequena parte dos números que estão no seu cartão (normalmente tem de introduzir 3 números). O seu banco também não lhe pede que instale uma aplicação no telemóvel para reforçar a segurança das suas operações. Estas aplicações são, tipicamente, vírus.

Em caso de dúvida, telefone para o seu banco para confirmar que ação deve tomar.

Verifique regularmente os movimentos da sua conta bancária e dos seus cartões de crédito. Se algum movimento for suspeito, deve alertar de imediato o seu banco e a Polícia Judiciária através do contato telefónico do serviço de piquete disponível em www.pj.pt.

De um modo geral deve também evitar abrir anexos ou aceder a páginas de Internet que constem em emails de que desconfie. O simples facto de abrir uma página da internet ou um documento de texto pode infetar o seu computador com um vírus que envia as suas informações para os criminosos. Um endereço de email é facilmente falsificado e, portanto, não deve confiar num email simplesmente porque vem de uma determinada fonte. O remetente pode não ser quem parece.

Por último, deve ter sempre ativo e atualizado um antivírus e deve manter aplicações como o *Java* e o *Flash* atualizados. Embora o mais importante seja seguir as recomendações apresentadas anteriormente e ter uma atitude de precaução.

|  |
| --- |
| **Resumo** |
| * **O seu banco nunca entra em contacto consigo via email para lhe pedir informação**
* **Não aceda a páginas da Internet nem a anexos que estejam em emails estranhos**
* **Mantenha o antivírus e aplicações como Java e Flash atualizados**
* **Em caso de dúvida contacte o seu banco telefonicamente para confirmação**
 |

---------------------------------------------------------------------------

**Mês Europeu da Ciber-Segurança**

Este artigo é da autoria de especialistas do CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática (www.cert.pt) da FCCN-Fundação de Computação Científica Nacional (www.fccn.pt/pt) e insere-se na campanha "Uma dica por dia" integrada no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013.

O Mês Europeu da Ciber-Segurança é uma iniciativa da ENISA - Agência Europeia para a Segurança das Redes e Informação (www.enisa.europa.eu) e o seu objectivo é informar os utilizadores sobre a importância da segurança da informação, bem como demonstrar algumas medidas simples para proteger os seus dados.

------------------------------------------------------------------------------

**Nota aos editores da Imprensa regional**

Os artigos da autoria dos técnicos do CERT.PT incluídos no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013, surgem no site da Ciência na Imprensa Regional numerados, de forma a permitir a sua mais fácil identificação. No entanto, eles são absolutamente independentes uns dos outros e podem ser publicados pelos órgãos de comunicação de forma avulsa.

------------------------------------------------------------------------------

Foto de Rudyanto Wijaya

(Existem ficheiros de imagem de mais alta resolução disponíveis para download)

