BANCO DE PORTUGAL
EUROSISTEMA

PAGAMENTOS NA INTERNET
Boas Práticas | Titulares de cartões

Antes de realizar pagamentos na Internet, leia cuidadosamente as condições gerais de utilização do cartão que pretende utilizar. Caso persistam dúvidas, ou se necessitar de mais informação sobre os cuidados e procedimentos a adotar, solicite tais esclarecimentos diretamente ao emitente do cartão em causa (instituição de crédito, instituição de pagamento ou instituição de moeda eletrónica emitente).

A execução de um pagamento com cartão na Internet implica a divulgação de dados desse cartão. Por isso, deve tomar algumas medidas de segurança para evitar situações de fraude:

- Utilize cartões de pagamento com características de segurança acrescida, tais como ter um saldo/*plafond* limitado, uma reduzida data de validade ou procedimentos de autenticação adicionais (exemplos: cartões pré-pagos ou 3D secure, ou MB NET);

- Não divulgue a sua informação confidencial/pessoal (exemplos: palavras-passe, dados de documentos de identificação pessoal ou dados do cartão de pagamento), a menos que tal seja imprescindível para a realização do pagamento e sempre em sítios da Internet que lhe ofereçam segurança. Esteja sempre atento a solicitações de dados pessoais ou de natureza fora do comum, ainda que provenientes de uma entidade aparentemente confiável;

- Evite utilizar acessos públicos e/ou computadores partilhados para efetuar pagamentos na Internet (exemplos: cibercafés, centros comerciais, aeroportos ou hotéis);

- Proteja as comunicações sem fios (WiFi) através da adoção de protocolos seguros, tais como WPA2-PSK e WPA-TKIP, e evite a utilização de *hotspots* públicos. Saiba mais, consultando o seu fornecedor do serviço de acesso à Internet;

- Não utilize a mesma palavra-passe para todos os sítios da Internet. Utilize palavras-passe fáceis de memorizar, mas difíceis de adivinhar por terceiros. Evite utilizar palavras-passe demasiado óbvias (exemplos: 123456 ou ABCDEF) ou associadas a informação pessoal fácil de obter (exemplos: datas de aniversário ou nomes). As palavras-passe são pessoais e intransmissíveis. Evite escrevê-las em papéis, não as divulgue a terceiros, nem as envie por *email* ou telemóvel;

- Instale um antivírus no seu computador/*tablet*/*smartphone* (apenas recorrendo a programas originais). Mantenha o antivírus e os restantes programas sempre atualizados;

- Proteja as suas comunicações utilizando uma *firewall*, para que possa filtrar o tráfego da Internet;

- Efetue apenas pagamentos a entidades credíveis (que conheça e nas quais confie) e em sítios seguros (cujo endereço comece por HTTPS://). A letra 'S' indica que a ligação ao serviço *online* da instituição é segura. Outro elemento de segurança é dado pela existência do símbolo de um cadeado na barra inferior ou superior da janela do sítio da Internet;

- Procure informações sobre a referida entidade na Internet. Para confirmar a credibilidade da entidade faça uma pesquisa pela respetiva designação através de motores de busca. Obtenha referências de amigos e familiares que possam já ter efetuado compras a essa entidade ou procure, por exemplo, em fóruns de discussão, confirmando a inexistência de reclamações recorrentes sobre a mesma;

- Verifique o endereço físico da entidade, ou seja, se existem contactos de telefone, *email*, fax, etc. Tenha atenção especial com sítios que só apresentem contactos de telemóveis;

• Guarde sempre os registos das transações efetuadas *online*, incluindo a informação da entidade e o endereço do seu sítio da Internet. Sempre que possível faça o *printscreen* dos dados da operação. Verifique regularmente o seu extrato de conta e confirme se os movimentos realizados com o seu cartão foram devidamente registados e se os valores estão corretos;

• Observe os procedimentos e os cuidados acordados e/ou recomendados pelo emitente do cartão para a realização de pagamentos na Internet;

• Comunique ao emitente do cartão, assim que possível, a perda, o roubo ou qualquer situação suspeita referente a esse cartão, utilizando os contactos disponibilizados pelo emitente, bem como os contactos divulgados para esse efeito no *site* do Banco de Portugal:

https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/contactosdosemissorescartoes.pdf;

• Seja cauteloso perante ofertas irrecusáveis ou pechinchas, pois, frequentemente, correspondem a situações de fraude;

• Ignore os *links* e anexos em *emails* suspeitos ou dos quais não conheça a fonte. Considere suspeitos os *emails* redigidos numa linguagem desapropriada/despropositada, cujo teor lhe seja alheio ou não faça sentido, ou que tenham uma formatação gráfica dúbia, mesmo que provenha de fonte fidedigna (esta poderá ter sido alvo de manipulação). Muitas vezes os *links* e os ficheiros anexos que constam nesses *emails* instalam programas maliciosos, que põem em causa a confidencialidade dos seus dados;

• Evite aceder a sítios da Internet a partir de *links*. Insira diretamente o endereço de acesso (URL) pretendido no *browser*. Se aceder a determinado sítio da Internet a partir de um *link* valide a correspondência entre a designação do serviço e o endereço de acesso.

Glossário técnico

O serviço MB NET é um serviço disponibilizado pela SIBS que permite criar um cartão de pagamento virtual assente em determinados dados de um cartão de pagamento real. Possibilita a realização de compras na Internet sem fornecer o número do cartão de pagamento real e os demais dados normalmente solicitados (nome do titular do cartão, data de validade e códigos CVV2/CVC2/3CSC).

O protocolo 3D-Secure (*Verified by Visa* da Visa, *SecureCode* da MasterCard ou *SafeKey* da American Express) permite verificar se a pessoa que está a efetuar a transação na Internet é um titular autorizado. Este protocolo pode ser utilizado nas transações de comércio eletrónico com cartões de pagamento se o comerciante/aceitante o tiver implementado e se o cartão tiver essa funcionalidade disponível.

As *firewalls* permitem controlar os dados transferidos entre sistemas de uma infraestrutura. A sua implementação visa prevenir a intrusão nos sistemas de atividade maliciosa e evitar que informações sensíveis sejam transmitidas das para outros sistemas de forma não autorizada.

Saiba mais

Para informação adicional sobre as fraudes mais comuns utilizando o correio eletrónico, pode consultar o "Portal Todos Contam".

http://www.todoscontam.pt

Sobre recomendações de boas práticas para realização de pagamentos na Internet dirigidas a aceitantes e emitentes de cartões, pode consultar a informação disponível no *site* do Banco de Portugal.

https://www.bportugal.pt/page/sistemas-de-pagamentos-boas-praticas

Para mais informação sobre o Serviço MB NET consulte o *site* do seu banco ou do MB Way.