



# PAGAMENTOS NA INTERNET

## Boas Práticas | Aceitantes e emitentes de cartões

Os cartões de pagamento, designadamente cartões de crédito, cartões virtuais e cartões pré-pagos, são instrumentos com cada vez maior aceitação no comércio de bens e serviços através da internet.

Por isso, dedique particular atenção aos aspetos de segurança na realização de pagamentos nos sítios eletrónicos:

- Atualize regularmente o *software* utilizado com as últimas versões disponíveis. Instale apenas cópias legais de *software*. As atualizações de segurança nos sistemas operativos e nas aplicações utilizadas aumentam a proteção contra novas vulnerabilidades que sejam entretanto descobertas;
- Utilize programas antivírus originais e de comprovada idoneidade e eficácia, mantendo-os permanentemente atualizados, de forma a detetar e eliminar *malware* (intrusão de vírus). A propagação dos vírus pelos sistemas é normalmente veiculada através das redes (internas e externas) ou através de dispositivos de armazenamento de informação (exemplos: *pen drives* ou discos externos);
- Utilize *firewalls* restritivas, de forma a filtrar o tráfego, prevenir a intrusão de atividades maliciosas nos seus sistemas e evitar que informações críticas sejam transmitidas para outros sistemas de forma não autorizada;
- Execute periodicamente testes de intrusão nos seus sistemas informáticos (*Hacking Ético*). Estes testes visam simular um ataque de uma fonte maliciosa, de forma a identificar vulnerabilidades dos sistemas informáticos, para, posteriormente, desenvolver medidas preventivas adicionais;
- Proteja-se contra ataques de negação de serviço (*DoS – Denial of Service*). Devem ser implementados mecanismos adequados de proteção (exemplos: filtragem de tráfego, filtragem de redundância e realiza-

ção de *backups* regulares de toda a informação crítica), de modo a impedir ataques *DoS*;

- Aplique boas práticas no desenvolvimento de aplicações web e na realização dos respetivos testes. Existem boas práticas já definidas que podem ser aplicadas, tais como as constantes das recomendações da *OWASP (Open Web Application on Security Project, www.owasp.org)*;
- Implemente um sistema de deteção e prevenção de intrusão na infraestrutura (*IDS - Intrusion Detection System*), de forma a bloquear acessos não autorizados (provenientes de *hackers, software* malicioso e / ou colaboradores mal intencionados). Este tipo de sistemas deve ser implementado em infraestruturas que contenham dados sensíveis;
- Implemente um sistema de deteção de fraude, que analise as transações em tempo real e alerte para situações suspeitas, com vista a mitigar o impacto das mesmas;
- Implemente um plano de resposta a incidentes que contemple os seguintes passos: (i) avaliação inicial; (ii) comunicação do incidente; (iii) contenção dos danos e minimização dos riscos; (iv) identificação do tipo e da gravidade do comprometimento; (v) notificação de entidades externas, se apropriado; (vi) recuperação dos sistemas; (vii) compilação da documentação do incidente; e (viii) correção das falhas identificadas;
- Adote protocolos seguros para proteger a confidencialidade e integridade dos dados. Estes protocolos devem abranger os sítios na internet (exemplo: *HTTPS*); transferência de ficheiros (exemplos: *SFTP, FTPS, SSH*); correio eletrónico (exemplos: *PGP* ou *S/MIME*); comunicações com fios (exemplo: *VPN* baseada no protocolo *IPSEC* ou *TLS*); e comunicações sem fios (exemplos: *WiFi* protegido com *WPA2 –* mínimo de 128 bits – e *EAP*);

- Não armazene dados confidenciais, tais como códigos de segurança (exemplos: CVV2, CVC2 e 3CSC) e dados de cartão (exemplos: número de cartão e data de expiração). Quando esse armazenamento seja necessário, os dados devem ser protegidos: podem ser truncados, sujeitos a funções irreversíveis criptograficamente seguras (*One-way hashes based on strong cryptography*), transformados em índices ou cifrados com algoritmos criptográficos fortes;
- Fomente a correta utilização de credenciais de acesso aos sistemas. Cada colaborador deve ter um acesso único e limitado às necessidades das suas funções. A utilização das credenciais de acesso deve ser registada e inspecionada regularmente. Em caso de ataque, deve ser possível investigar as situações de uma forma célere;
- Utilize palavras-passe fortes nos terminais de acesso e / ou nas aplicações de acesso aos sistemas de informação. As palavras-passe devem ter no mínimo 8 caracteres, conter maiúsculas, minúsculas, dígitos e caracteres especiais. Não devem conter o nome do utilizador nem ser usados isoladamente números, nomes, datas, palavras, marcas, etc;
- Consciencialize os seus colaboradores para os assuntos de segurança, nomeadamente através da implementação de um programa pedagógico de segurança (*security awareness*), que promova a utilização de métodos adequados para tratar, transmitir, armazenar e destruir informação sensível. Instrua os seus colaboradores sobre as boas práticas que devem seguir;
- Fomente a utilização de cartões de segurança acrescida, tais como ter um saldo / *plafond* limitado, uma reduzida data de validade ou exigir procedimentos de autenticação adicionais (exemplos: cartões pré-pagos ou 3D secure, ou MB NET);
- Exija aos titulares de cartões a introdução de códigos de segurança aquando do pagamento *online* (exemplos: CVV2, CVC2 ou 3CSC). A utilização destes códigos é uma primeira linha de defesa contra ataques baseados na geração ou extrapolação de números de cartões;
- Adote um protocolo 3D-Secure como forma de autenticar o utilizador no momento do pagamento (*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;
- Divulgue previamente aos titulares dos cartões de pagamento as medidas de segurança que devem ser observadas na realização de pagamentos através da internet e os riscos inerentes a essas operações;
- Disponibilize as boas práticas para a realização de pagamentos na internet com cartões de pagamento aos respetivos titulares, nomeadamente através da prestação de informação nos seus sítios da internet;
- Implemente um canal seguro para troca de informação sensível com os seus clientes titulares de cartões e informe-os da existência do mesmo e do respetivo modo de funcionamento. Os clientes devem ser esclarecidos dos métodos indicados para a deteção de eventuais comunicações fraudulentas com a aparência de terem origem no prestador de serviços. Os clientes devem ainda ser informados dos procedimentos adequados para a denúncia de fraudes e do modo pelo qual o seu prestador de serviços lhes comunicará a eventual ocorrência de ataques fraudulentos;
- Implemente soluções que possibilitem a auditabilidade dos acessos e transações.

## 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 transferi-

dos entre sistemas de uma infraestrutura. A sua implementação visa prevenir a intrusão nos sistemas de atividade maliciosa e evitar que informa-

ções sensíveis sejam transmitidas 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".

[www.todoscontam.pt](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 Portal do Cliente Bancário.

[www.clientebancario.bportugal.pt](http://www.clientebancario.bportugal.pt)

Para mais informação sobre o Serviço MB NET

consulte o respetivo sítio da internet.

[www.mbnet.pt](http://www.mbnet.pt)

Para mais informação sobre o protocolo 3D-Secure, consulte o Adquirente / Acquirer.