

PLANO NACIONAL  
DE FORMAÇÃO FINANCEIRA



## PAGAMENTOS NA INTERNET

Os cartões podem ser usados para pagamentos através da internet. Esta possibilidade está, normalmente, disponível para cartões de crédito ou cartões de débito, através da divulgação de dados do cartão. Para evitar problemas de **fraude** ([/fraude-informatica](#)), devem ser tomadas medidas de segurança, verificando por exemplo se a página de internet onde está a ser realizado o pagamento é segura.

Estão disponíveis na internet alguns serviços que oferecem maior segurança nos pagamentos *online* com cartões. Estes serviços permitem efetuar pagamentos *online*, sem divulgar os dados do cartão ou da conta bancária em que serão debitados esses pagamentos.

Para aderir a estes serviços, o cliente tem de se registar no sítio de internet da instituição que disponibiliza esses serviços e, nalguns casos, de solicitar também a adesão junto da sua instituição de crédito. Os dados do cartão de crédito ou débito que serão usados para realizar compras *online* são divulgados apenas a estes sítios e de forma segura.

Com base nestes dados, alguns destes serviços geram um cartão de crédito virtual que o cliente utiliza para fazer as compras *online* na página de internet que pretende. A utilização deste cartão virtual pode ser limitada a um único pagamento, durante um prazo de tempo curto, como por exemplo um mês, e o cliente pode definir um montante limite igual ao pagamento que pretende realizar com o cartão. O risco de fraude é minimizado pelo facto do cliente efetuar as compras *online* com um cartão virtual temporário de *plafond* limitado, em vez de divulgar o número do seu cartão bancário.

Noutros casos, os dados do cartão de crédito são usados para criar uma conta virtual em nome do cliente. Esta conta é depois usada pelo cliente para realizar as suas compras *online*, sem divulgar o número do seu cartão de crédito. Em vez de associar um cartão de crédito à sua conta virtual, o cliente pode ainda transferir dinheiro para essa conta e utilizar o saldo para fazer compras *online*. A utilização desta forma de pagamento só é possível em sítios de internet que aceitem este tipo de conta.

## CUIDADOS ESPECIAIS A OBSERVAR EM PAGAMENTOS NA INTERNET

### Quando faz a compra, opte por uma forma de pagamento segura

- Certifique-se de que apenas disponibiliza os dados necessários para concluir a compra;
- Opte, preferencialmente, por uma das seguintes formas de pagamento:
  - **Referência multibanco.** O comerciante envia uma SMS ou *e-mail* com os dados para efetuar o pagamento, dentro de determinado prazo, num caixa automático ou através do *homebanking*;
  - **Instrumentos de pagamento com segurança acrescida.** Prefira utilizar cartões com um limite de crédito (plafond) limitado, um reduzido prazo de validade ou com procedimentos de autenticação adicionais (procedimentos que permitam a autenticação forte do cliente);
  - **Cartões virtuais.** Um cartão virtual é um cartão gerado e utilizado em contexto eletrónico. No momento da compra, não há divulgação dos dados do cartão real, o que introduz maior segurança na operação. A aplicação MB WAY, por exemplo, permite gerar cartões virtuais MB NET e efetuar as mesmas operações sem nunca divulgar os dados reais do seu cartão de pagamento.

## AUTENTIFICAÇÃO FORTE DO CLIENTE

Procedimento de autenticação no qual o cliente, a pedido da instituição, utiliza dois ou mais dos seguintes elementos:

- Algo que só o cliente conhece – por exemplo, uma palavra-passe, um código, um número de identificação pessoal (PIN);
- Algo que só o cliente possui – por exemplo, um dispositivo de autenticação (*token*), um cartão inteligente, um telemóvel;
- Algo do próprio cliente – por exemplo, uma característica biométrica, designadamente uma impressão digital.

Estes elementos têm de ser independentes, isto é, a violação de um deles não deve comprometer a fiabilidade do(s) outro(s). Além disso, pelo menos um destes elementos deve ser não reutilizável e não reproduzível (com exceção da característica inerente ao cliente) e insuscetível de ser furtado através da internet.

Da utilização destes elementos resulta um código de autenticação. Nos casos em que é legalmente exigida a autenticação forte do cliente, o cliente deve usar o código de autenticação para validar a operação de pagamento que pretende efetuar.

Por exemplo, ao abrigo deste mecanismo de autenticação mais robusto, é exigido ao cliente bancário, aquando da realização de uma compra com cartão através da internet, que, além de indicar os elementos do seu cartão de pagamento, insira um código irrepitível que lhe seja fornecido por mensagem escrita de telemóvel (SMS). Neste caso, o cliente bancário terá de ter previamente associado o seu número de telemóvel ao cartão.

## LINKS ÚTEIS RELACIONADOS

**Portal do Cliente Bancário> Canais digitais> Cuidados a ter** (<https://cliente bancario.bportugal.pt/pt-pt/cuidados-ter-na-utilizacao-de-canais-digitais>)

**Campanha de educação financeira digital #ficaadica (Youtube)** (<https://www.youtube.com/watch?v=QUJWUBXCBgQ>)

---

© Plano Nacional de Formação Financeira - Todos Contam