PAGAMENTOS NA INTERNET
Boas Práticas | Titulares de cartões

Desde 14 de setembro de 2019[1], os prestadores de serviços de pagamento (PSP) têm de efetuar autenticação forte do cliente (*strong customer authentication* – SCA) sempre que estes acedem *online* à sua conta, iniciam um pagamento eletrónico ou realizam uma ação remota que possa envolver risco de fraude no pagamento ou outros abusos. A aplicação de SCA implica que o PSP solicite ao utilizador pelo menos dois elementos de segurança, de que são exemplos um código enviado por SMS, um elemento biométrico (impressão digital ou reconhecimento facial) ou uma palavra-passe.

Os requisitos de SCA visam tornar as operações de pagamento mais seguras. Poderá consultar mais informação sobre as regras de SCA no sítio do Banco de Portugal: https://www.bportugal.pt/page/autenticacao-forte?mlid=3417.

Antes de realizar pagamentos com cartão 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, designadamente para perceber quais os mecanismos de SCA que o emitente do cartão em causa (instituição de crédito, instituição de pagamento ou instituição de moeda eletrónica) disponibiliza, informe-se junto do mesmo.

Pagamentos com cartão na Internet

A execução de um pagamento com cartão na Internet implica a utilização de informação sensível. 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;
- Assegure que o serviço 3D *Secure* do seu cartão de pagamento está ativo. Caso não esteja, solicite a adesão/ativação junto do seu banco ou prestador de serviços de pagamento. O serviço é gratuito e permite a utilização segura do cartão em lojas *online* aderentes aos sistemas "Verified by Visa" ou "MasterCard SecureCode" e "SafeKey" da American Express. Neste caso, quando efetuar uma compra, ser-lhe-á, por norma, pedido que realize SCA. Em Portugal, a solução mais comum para SCA de operações *online* com cartão é a validação da operação na *app* do seu banco ou prestador de serviços de pagamento. Informe-se junto do emitente do cartão sobre quais os mecanismos de SCA disponíveis;
- Não divulgue a sua informação confidencial, como 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;
- Nunca divulgue informação personalizada e sensível, como por exemplo a palavra-passe ou os códigos enviados por SMS para autenticação das operações. Adicionalmente, leia sempre, atentamente, o conteúdo dessas mensagens e confirme que a informação respeitante à transação está correta. Caso não reconheça a transação contacte imediatamente o emitente do cartão através dos canais habituais;
- Desconfie de contactos, por email ou por telefone, a informar que o seu acesso aos canais do seu banco ou prestador de serviços de pagamento, como por exemplo o *homebanking*, se encontram bloqueados, pois tal poderá corresponder a uma situação de fraude;
- Se receber uma chamada de um desconhecido, não assuma que esta é genuína apenas por este estar na posse dos seus dados pessoais básicos. Esta informação poderá ser encontrada *online* (por ex. redes sociais);

[1] Data de entrada em aplicação do Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 (Diretiva de Serviços de Pagamento revista, ou DSP2).

- Evite utilizar acessos a redes públicas e/ou computadores partilhados para efetuar pagamentos na Internet (como por exemplo, 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, e preferencialmente que conjuguem caracteres maiúsculos, minúsculos e numéricos. Evite utilizar palavras-passe demasiado óbvias (exemplos: 123456 ou ABCDEF) ou associadas a informação pessoal fácil de obter (como por exemplo, 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* e para isso apenas recorra a programas originais. Mantenha o antivírus e os restantes programas sempre atualizados. Adicionalmente, pode aderir a serviços de VPN para obter um maior grau de segurança;
- Proteja as suas comunicações utilizando uma *firewall*, para que possa filtrar o tráfego da Internet. 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 para outros sistemas de forma não autorizada;
- 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 provenham de fonte fidedigna, uma vez que esta fonte 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;
- 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 a entidades que só apresentem contactos de telemóveis;
- Seja cauteloso perante ofertas irrecusáveis ou pechinchas, pois, frequentemente, correspondem a situações de fraude;
- 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 ou os contactos divulgados para esse efeito no sítio do Banco de Portugal:

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

Saiba mais

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

https://www.todoscontam.pt/

Sobre os cuidados a ter para prevenir fraudes *online*, veja o vídeo disponível no site do Banco de Portugal.

https://www.bportugal.pt/comunicado/banco-de-portugal-divulga-video-sobre-cuidados-ter-para-prevenir-fraudes-online

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