



MAIO 2017 Nº 79

English version



A revisão da Diretiva de Meios de Pagamento (PSD2 (EU) 2015/236), mandou a Autoridade Bancária Europeia, em cooperação com o Banco Central Europeu, a definir os requisitos para um sistema de Autenticação Forte de Clientes ainda mais robusto por forma a salvaguardar os dados pessoais bem como o património financeiro dos utilizadores de serviços de pagamentos *online*.

Assim, os utilizadores de serviços de pagamentos irão assistir a uma evolução gradual tanto na validação de acessos, como na autenticação de operações registadas *online*.

O procedimento de autenticação forte permite verificar a identidade de um Cliente ou de uma entidade e é baseado na combinação de dois (ou mais) dos seguintes elementos:

- Algo que apenas o utilizador conhece, por exemplo, uma palavra-passe, um código, um número de identificação pessoal;
- Algo que apenas o utilizador possui, por exemplo, um dispositivo de autenticação (token), um cartão bancário, um telemóvel, e;
- Uma característica inerente ao utilizador, por exemplo, uma característica biométrica como uma impressão digital, voz, retina, etc.

Os elementos escolhidos devem ser independentes, isto é, a violação de um não pode comprometer a segurança do(s) outro(s). Além disso, um destes elementos não pode ser reutilizável, nem reproduzível (com exceção da inerência), nem suscetível de ser roubado através da Internet.

As formas de autenticação baseadas nos elementos acima mencionados podem assumir várias formas.

Desde os já conhecidos e implementados na maioria dos serviços de homebanking nacionais, como por exemplo: o Código de

Autorização enviado por SMS ou o dispositivo Token que funciona em conjunto com um cartão bancário; como os que estão a surgir em várias plataformas baseados no Cartão de Cidadão ou em dados biométricos.

Falando no Cartão de Cidadão. Sabe qual é a funcionalidade do chip que este tem incorporado? O chip permite confirmar, de forma segura, a identidade do titular no acesso a portais e sites de diferentes entidades públicas. Contudo, para poder usar este método de autenticação é necessário que tenha um PIN e um leitor de cartões.

O procedimento de autenticação forte deve também ser concebido de forma a proteger a confidencialidade dos dados.

Para evitar a obrigação de autenticar todas as operações registadas no homebanking, estão previstas algumas isenções ao Sistema de Autenticação Forte, nomeadamente, a definição de beneficiários frequentes, as transferências permanentes e alguns pagamentos de baixo valor (até a um limite acumulado definido).

Assim, comece já a definir a sua lista de Favoritos (beneficiários frequentes) em millenniumbcp.pt, no menu:

- “Área M”, opção “Favoritos: Criar”, caso o seu acesso seja efetuado pela área de Particulares;
- “Outros serviços”, opção “Gestão de Beneficiários”, caso o seu acesso seja efetuado pela área de Empresas.

Para mais informações sobre credenciais de validação e autenticação, sugerimos que consulte o artigo “Perguntas Frequentes sobre os Códigos de Acesso e Códigos de Autorização nos canais”, disponível na nossa página de Segurança, em “M - Tudo sobre: Segurança”.

LEMBRE-SE QUE...



No acesso ao *homebanking* do Millennium bcp **NUNCA solicitamos o seu número de telemóvel ou a instalação de software/programas de segurança.**

Aproveitamos a oportunidade para alertar para o conteúdo da mensagem fraudulenta detetada recentemente, a qual afeta o equipamento do utilizador e, por consequência, altera as páginas de acesso ao site do millenniumbcp.pt

Exemplo da mensagem fraudulenta:

1. Panasonic Viera Smart TV UHD
4K HDR 580X786 146cm
4K UHD
1 667,00 €

Portes 16,79 €

PAGAMENTO

Valor Total com IVA 1 683,79 €

Meio de Pagamento **Mastercard**

Quer saber mais sobre o pagamento da sua encomenda, serviços pós-venda, devoluções, devoluções, consulte a Ajuda ou utilize o nosso formulário de contacto. Também poderá contactar-nos através do número 707 31 34 35 (todos os dias, das 9h às 19h) ou por e-mail: ajuda@vodafone.pt (rede fixa: 0,122€/min IVA incluído | Rede Móvel: 0,3096€/min IVA incluído).

Se quiser a sua encomenda.

[A minha Conta](#)

EXPEDIÇÃO

Endereço de Expedição
[Verificar](#)

Endereço de Faturação
[Verificar](#)

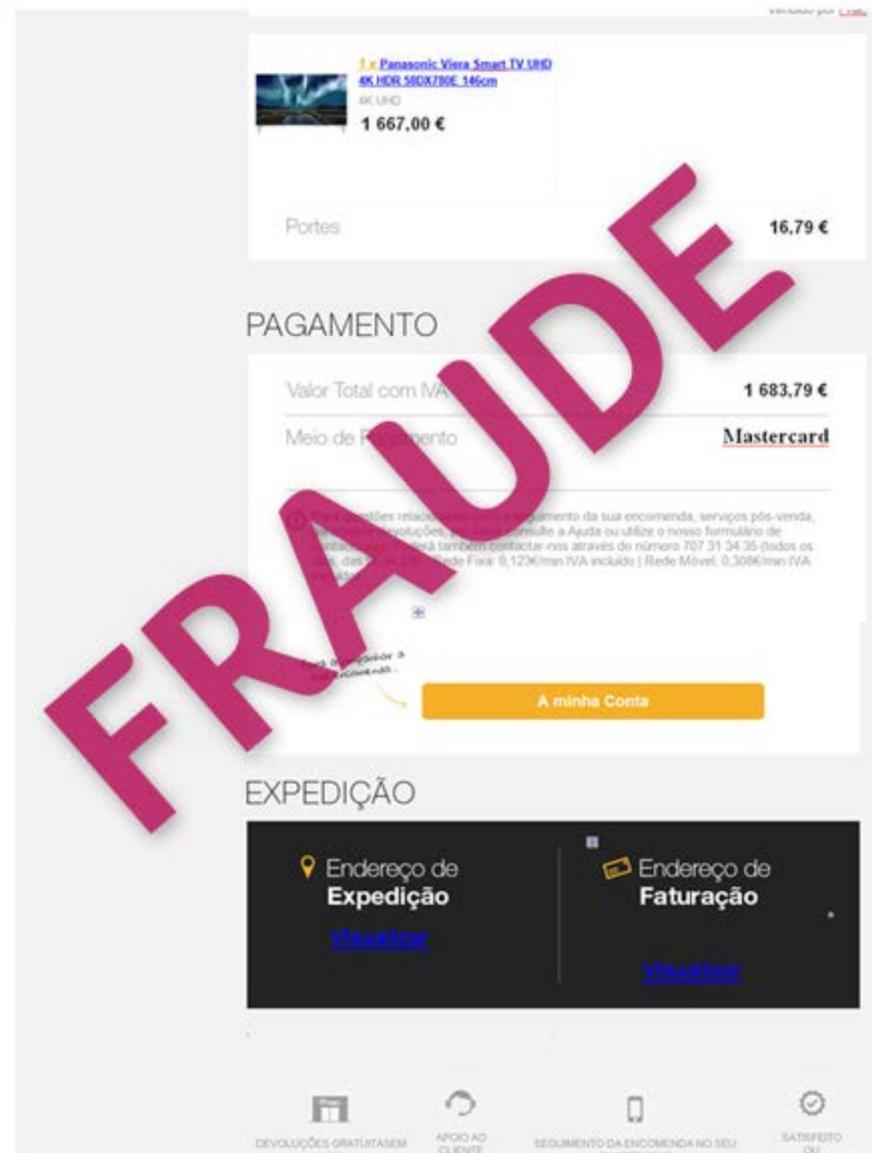
DEVOLUÇÕES GRATUITAS EM 15 DIAS

APOIO AO CLIENTE

SEGUIMENTO DA ENCOMENDA NO SEU COMPUTADOR

SATISFEITO OU NÃO

FRAUDE



Recordamos que:

- Deve suspeitar de qualquer mensagem de correio eletrónico que peça uma “ação imediata” ou crie um senso de urgência, que contenha erros ortográficos/gramaticais e anexos de ficheiros executáveis (.exe);
- Os três dígitos aleatórios do Código de Acesso Multicanal são-lhe solicitados no acesso (login) a www.millenniumbcp.pt bem como na manutenção dos seus dados pessoais/credenciais de acesso (caso erre a introdução das posições, estas mantêm-se até que o login seja efetuado com sucesso);
- Leia atentamente o conteúdo dos SMS’s recebidos com Códigos de Autorização, dado que os dados da operação são identificados no texto do SMS;
- O Phishing visa confirmar/obter, de forma abusiva, dados pessoais/credenciais de acesso através de mensagens com *links*/anexos que podem infetar o computador com software malicioso ou conduzir o utilizador a sites falsos, idênticos aos fidedignos. Evite seguir *links* para sites externos, bem como abrir ficheiros executáveis;
- Analise as mensagens de correio eletrónico que recebe antes de abrir, confirmando sempre a origem e o assunto da mesma e, se continuar com dúvidas, confirme junto da entidade emitente;
- Nunca faculte informação ou elementos de carácter pessoal como resposta a uma mensagem de correio eletrónico;
- Instale (caso ainda não o tenha feito) um *software* antivírus no seu computador e efetue regularmente as atualizações do mesmo.

Lembre-se que a proteção dos seus dados, património, computador e equipamentos móveis depende de si!

SERVIÇO DE ALERTAS QUER ESTAR SEMPRE INFORMADO?



siga-nos no facebook



Esta informação é da responsabilidade do Millennium bcp.

Este e-mail é apenas informativo, por favor não responda para este endereço. Para obter esclarecimentos adicionais, sobre este ou qualquer outro assunto, ou efetuar sugestões, e para que o possamos servir melhor e mais eficazmente, sugerimos que visite o site do Millennium bcp ou ligue para o número de telefone 707 50 24 24 (Atendimento Personalizado 24 horas).

Se ligar para 707 50 24 24 a partir da rede fixa terá um custo máximo de 0.10 € por minuto; se optar por nos ligar a partir da rede móvel o custo máximo por minuto será de 0.25 €. A estes valores acresce o respetivo IVA.

Estes e-mails não permitem o acesso direto ao site do Millennium bcp, não incluem atalhos (links)*, nem são utilizados para lhe solicitar quaisquer elementos identificativos, nomeadamente códigos de acesso. Se receber um e-mail, aparentemente com origem no Millennium bcp, que não esteja de acordo com esta informação, não responda, apague-o e comunique, de imediato, este facto para: [informacoes.clientes @ millenniumbcp.pt](mailto:informacoes.clientes@millenniumbcp.pt).

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço eletrónico, aceda ao Homebanking no site do Millennium bcp e, no menu "Área M", seleccione a opção "Criar / Alterar e-mail".

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 5.600.738.053,72 euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa coletiva 501 525 882.

* Alguns serviços de e-mail assumem, automaticamente, links em certas palavras, sem qualquer responsabilidade por parte do Millennium bcp.

Versão portuguesa



STRONG AUTHENTICATION OF CLIENTS

The revision of the Directive on Payment Services (PSD 2 Directive (EU) 2015/2366) empowered the European Banking Authority, in cooperation with the European Central Bank, to define the requirements for a more robust Strong Authentication System for Customers so as to safeguard personal data and the financial assets of users of payment services online.

Thus, the users of payment services are going to experience gradual evolution in both the validation of accesses and in the authentication of online transactions.

Strong authentication enables verification of the identity of a Client or entity and is based on the combination of two (or more) of the following elements:

- Something only the user knows, for instance, a password, code, personal identification number;
- Something only the user has, for example, an authentication device (token), a bank card, a mobile phone; and
- An inherent feature of the client, a biometric feature such as a finger print, voice, retina, etc.

The elements chosen must be independent, i.e. the breach of one cannot compromise the other element(s) security. In addition, one of these cannot be reused or reproduced (except for the inherent feature), or susceptible of being stolen online.

The forms of authentication based on the aforementioned elements may take on different forms.

From the best known and implemented in the majority of Portuguese online banking services, such as: the Authorization Code sent via text message or the Token device that works together with a bank card, to the ones coming out now in various platforms, based on the citizen card or on biometrics.

Regarding the Citizen Card, do you know what the microchip in it is for? The chip enables secure confirmation of the identity of the holder when accessing portals and websites of various public entities. Yet, to be able to use this authentication method, you must have a PIN code and a card reader.

The strong authentication procedure must also be designed so as to ensure confidentiality of the data.

To avoid the need to authenticate every transaction made online, some exemptions to the Strong Authentication System are allowed, namely the definition of frequent beneficiaries, permanent transfers and some low value payments (up to a defined accrued limit).

This way, you can start defining your Favourites (frequent beneficiaries) at millenniumbcp.pt, under:

- “M Area”, choose “Favourites: Create”, if you access it through the Individuals website;

- “Other services”, choose “Manage Payees”, if you access it through the Corporate website;

For further information on validation and authentication credentials, we suggest reading the articles available on our security page, at “M - All about: Security”.

Source: Millennium bcp

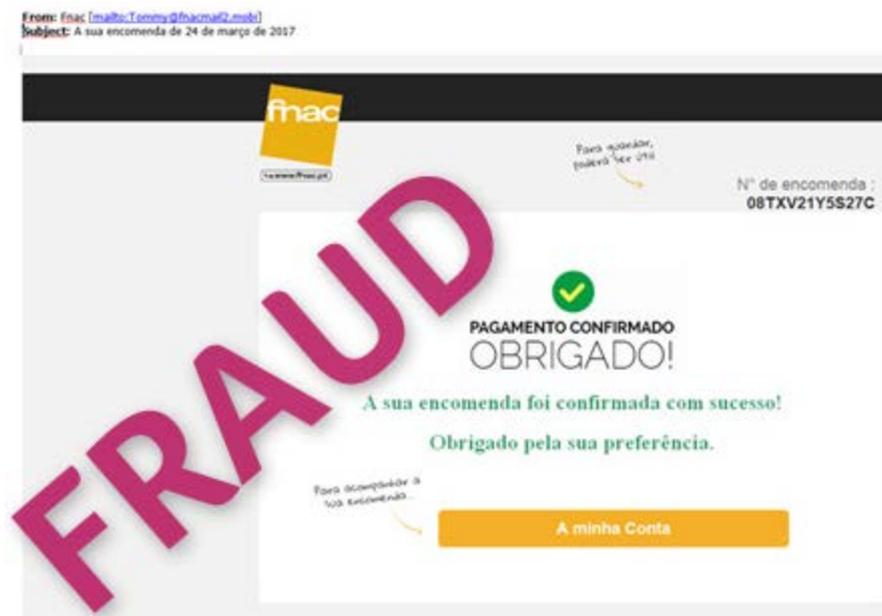
REMEMBER...

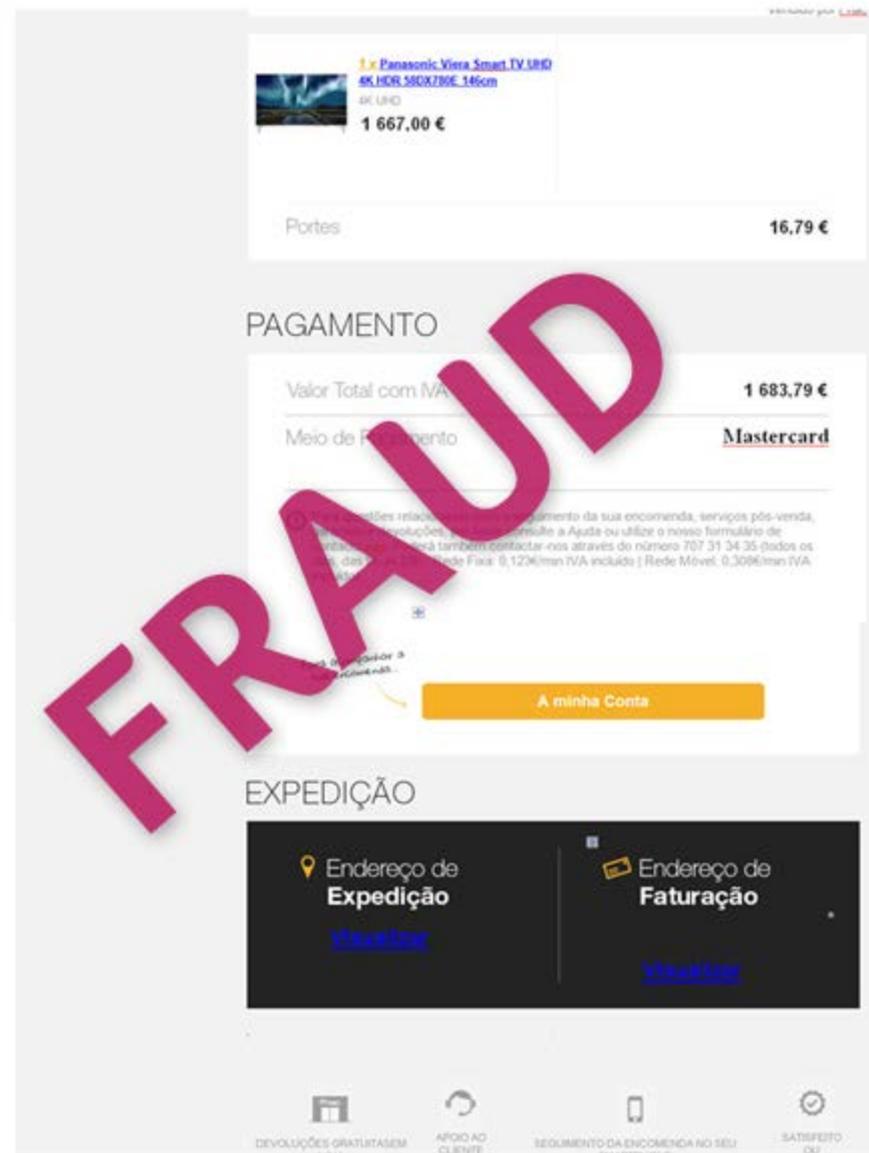
M

To access Millennium bcp's homebanking services, the Bank **NEVER requests your mobile phone number or the installation of security software.**

We also take this opportunity to warn you about the contents of a fake message recently found that tampers with the user's device and therefore alter the pages that open the millenniumbcp.pt website.

Example of the e-mail received:





Please be reminded that:

- You should beware of any e-mail that requires "immediate action" or creates a sense of urgency, shows spelling errors or bad grammar and has attached executable files (.exe);
- The three random digits of the Multichannel Access Code are requested when you login to www.millenniumbcp.pt as well as for the management of your personal data/access codes (if you enter a wrong number, the three random positions requested remain the same until you login successfully);
- Carefully read the SMS received containing the Authorisation Codes since the transaction data are identified in the SMS;
- Phishing aims to abusively confirm/get personal data/access codes through messages with links/attachments that can infect a computer with malicious software or lead the user to fake websites, identical to the trustworthy websites. Avoid opening links to external websites as well as opening executable files;
- Analyse the e-mails you receive before opening them, always confirming the source and the subject, if possible, with the issuer;
- Never provide personal information or data in an e-mail reply;
- Install (if you haven't done so yet) an antivirus software and update it regularly.

Remember: the protection of your data, assets, computer and mobile devices depends on you!

Millennium bcp is responsible for this information

This is an automated notification. Please do not reply to this message. We're happy to help you with any questions or concerns you may have and listen to your suggestions. So that we can provide you best service, please go to the Millennium bcp website or dial 707 50 24 24.

If you call 707 50 24 24 using the landline you will pay a maximum of 0.10 € per minute; if you choose to call us using a mobile phone, the maximum cost per minute will be of 0.25 €. These charges are subject to VAT.

These e-mails do not grant direct access to the Millennium bcp website, nor do they include links*, nor are they sent to ask for any personal details (namely access codes). If you do receive any such e-mail, apparently sent by Millennium bcp but not in accordance with the above information, do not reply: delete and report it immediately to: [informacoes.clientes @ millienniumbcp.pt](mailto:informacoes.clientes@millenniumbcp.pt)

If you do not wish to receive such information via e-mail or if you wish to change your e-mail address, please go to the Millennium bcp Homebanking, then chose "Customize/Email" in the menu option "M Area".

Banco Comercial Português, S.A. Company open to public investment Registered Office: Praça D. João I, 28 - Porto. Share Capital: 5.600.738.053,72 euros Registered at the Companies Registry Office of Oporto. Single registration and tax identification number 501 525 882.

* Some mail services will, automatically, assume certain words as links, without any liability from Millennium bcp.