

AGOSTO 2017 Nº 80

English version



Porque a segurança é uma das nossas prioridades, o site do Millennium bcp disponibiliza informação indispensável relativamente ao acesso e à utilização destes canais, bem como formas que possibilitam um acompanhamento dos acessos e dos movimentos que afetam o seu património e, eventuais, ataques de phishing.

Temos uma equipa totalmente dedicada à segurança dos sistemas de informação.

Desenvolvemos mecanismos para responder às preocupações de segurança *online*, aplicando as medidas necessárias para prevenir os nossos utilizadores, monitorizar e evitar possíveis fraudes bancárias, suspendendo, se necessário, credenciais de acesso, por precaução, até esclarecimento junto do Cliente.

Implementámos um conjunto de medidas de segurança que nos ajudam a detetar e evitar acessos e registo de transações suspeitas. Esta análise só é possível com a **ajuda dos nossos Clientes e, inclusive, de não Clientes, que nos reencaminham e-mails suspeitos** com o objetivo de agilizar a identificação de softwares maliciosos e, assim, cooperar na redução de phishing.

O **envio trimestral desta Newsletter de Segurança** é uma das formas utilizadas para comunicar e alertar sobre temas de segurança.

Contudo, tem sempre disponível em www.millenniumbcp.pt:

- A **área de Segurança** totalmente dedicada a este tema, que pode consultar acedendo ao menu "M > Tudo sobre > Segurança".

- Sempre que identificamos um novo método de phishing, colocamos um aviso na página inicial do site com a descrição do método usado. Estes artigos contêm, sempre que possível, imagens das páginas falsas ou do conteúdo do *e-mail* fraudulento. Os **Avisos de Segurança** estão disponíveis para consulta na área de Segurança (menu "M > Tudo sobre > Segurança > Avisos de

segurança).

- Na página de acesso existem **recomendações para uma utilização segura**, conforme exemplo abaixo:

Acesso às contas



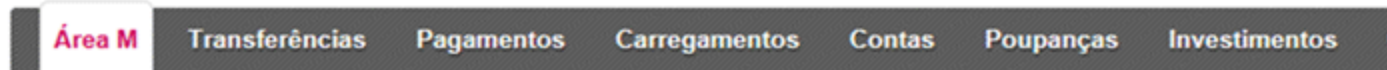
Recomendações de Segurança
No acesso ao homebanking **NÃO** solicitamos o nr. de telemóvel nem instalação de software →

e

Nunca digitar o Código de Acesso Multicanal completo.

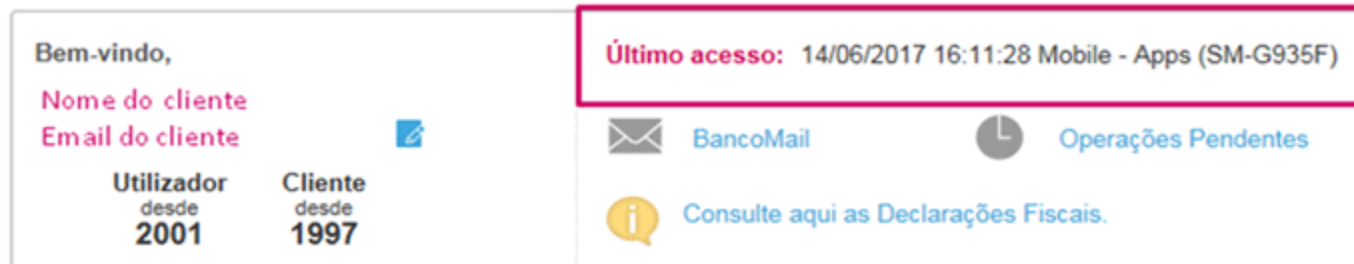
- Após login, e **ao fim de alguns minutos de inatividade, a sessão expira**. Não obstante existir este automatismo de segurança, termine sempre a sua sessão, na opção respetiva, "Terminar sessão", no canto superior direito.

- Após aceder ao site, é apresentada a **informação sobre o acesso anterior**: data, hora e canal. Desta forma, pode confirmar os acessos realizados, alertando o Banco sempre que detete situações suspeitas.



Área M Transferências Pagamentos Carregamentos Contas Poupanças Investimentos

A minha página



Bem-vindo,
Nome do cliente
Email do cliente ✉
Utilizador desde 2001
Cliente desde 1997

Último acesso: 14/06/2017 16:11:28 Mobile - Apps (SM-G935F)

✉ BancoMail ⌚ Operações Pendentes
i Consulte aqui as Declarações Fiscais.

(acesso à área de Particulares)

Bem-Vindo a Operações Bancárias



Bem-vindo (a),
Nome do cliente
Email do cliente ✉
Empresa

Último acesso: 2017/06/14 10:47:52

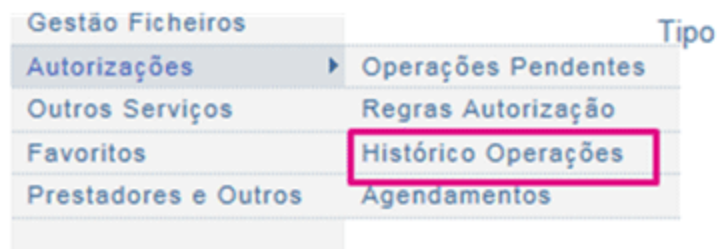
✉ BancoMail ver 0 mensagens novas
i Aviso de segurança: Alerta para mensagens fraudulentas.

(acesso à área de Empresas)

- A opção **Histórico de Operações** facilita a consulta, de uma forma célere, das transações registadas nos canais online, com as suas credenciais de acesso.



(acesso à área de Particulares)



(acesso à área de Empresas)

- O serviço de **Alertas** permite que o utilizador receba por email (gratuito) ou por SMS (sujeito a preçário) alertas sobre movimentos a débito ou a crédito que ocorram na(s) conta(s) de depósitos à ordem ou no(s) cartão(ões) de crédito.

Pode criar os seus Alertas através das seguintes opções:



(acesso à área de Particulares)

Outros Serviços |

Alertas

- › Extrato combinado (.pdf)
- › Nota de lançamento (.pdf)
- › Saldos e Movimentos
- › Débitos Diretos Europeus (SEPA)
- › Pagamentos e Transferências
- › Cartões
- › Cheques
- › Operações Documentárias
- › Anomalias no Processamento

(acesso à área de Empresas)

Alertamos, ainda, que:

- O Millennium bcp nunca envia **links** em mensagens de correio eletrónico (**e-mails**), por motivos de segurança;
- No acesso ao *homebanking* do Millennium bcp **NUNCA** solicitamos o número de telemóvel ou a instalação de **software/programas de segurança**. A janela abaixo (pop-up) é apresentada ao utilizador **no mais recente ataque de phishing, não disponibilize qualquer dado** e contacte-nos de imediato:

The banner features the Millennium bcp logo at the top. Below it, the title 'Ativação da App Proteção Antifraude' is displayed. A sub-headline reads: 'No sentido de melhorar a qualidade de serviço aos nossos clientes será necessário ativar a App Proteção Antifraude'. Below this, instructions state: 'Para iniciar a ativação do seu telemóvel aceder ao cadeado abaixo'. The visual elements include a hand holding a smartphone with a red 'X' and the word 'Desprotegido' on the screen, a red padlock icon, and a Millennium bcp Visa credit card. A large, diagonal watermark reading 'FRAUDE' is overlaid on the right side of the banner.

Se verificar alguma situação anómala em www.millenniumbcp.pt ou necessitar de esclarecimentos adicionais, por favor contacte-nos através do telefone 707 50 24 24 (Atendimento personalizado 24 horas).

Fonte: Millennium bcp

LEMBRE-SE QUE...



Caso esteja de férias, em viagem, no café ou mesmo na praia, é provável que através do seu computador portátil, *smartphone* ou *tablet* pretenda garantir a ligação à *Internet*.

Atualmente, o acesso a *wi-fi* público está em todo o lado através de *hotspots*.

Um *hotspot* público é uma rede sem fios, configurada para o acesso partilhado à *Internet*. O fornecedor do *hotspot* compra um ponto de acesso, liga-o à *Internet* e transmite o sinal num espaço público, permitindo que qualquer pessoa, com um dispositivo que esteja no alcance do sinal, possa aceder à rede e utilize a *Internet* gratuitamente.

Dado que a utilização de *hotspots* públicos é da responsabilidade do utilizador, deixamos-lhe algumas sugestões:

- Tenha atenção ao ambiente envolvente. Por definição, as redes *wi-fi* públicas não são seguras;
- Não permita que o seu dispositivo móvel se ligue automaticamente à rede mais próxima. Em vez disso, selecione manualmente o *hotspot* quando se ligar;
- Não efetue compras nem transações bancárias através de um *hotspot* público;
- Limite a troca de correio eletrónico e mensagens a comunicações casuais. Crie uma conta de correio eletrónico para utilizar em *hotspots* públicos;
- Desligue a rede móvel/dados móveis do seu dispositivo quando não os estiver a usar;
- Não use o mesmo código de acesso em *sites* diferentes. Sem se aperceber, pode disponibilizar o acesso às várias contas que detém;
- Certifique-se que tem um programa que o protege contra vírus, *malwares*, cavalos de tróia ou outros programas maliciosos e garanta que a atualização do mesmo é efetuada com a maior regularidade possível;
- Mantenha o sistema operativo e o antivírus permanentemente atualizado.

Os *hotspots* públicos podem ser úteis nas suas deslocações, desde que tome as devidas precauções.

Lembre-se que é da sua responsabilidade proteger o seu equipamento, os seus dados e a sua privacidade com boas ferramentas e uma utilização segura!

Fonte: Millennium bcp

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", selecione 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.



**SAFETY...
BECAUSE WE ARE
ALWAYS THINKING
OF YOU!**

Because safety is one of our priorities, Millennium bcp's website provides relevant information on the access and use of the channels, as well as on the ways enabling to monitor accesses, the entries impacting on your assets and eventual phishing attacks.

We have a team fully dedicated to the safety of the information systems.

We developed mechanisms to cope with online safety concerns by applying the measures needed to warn our users, monitor and prevent eventual bank frauds, suspending, if necessary and as a precaution, the access credentials, until all issues are clarified with the Client.

We implemented a set of safety measures which help us detect and avoid suspicious accesses and transactions. This analysis can only be made with the **help of our Clients and of, inclusively, non-Clients who forward to us all suspicious e-mails** in order to allow us to speed up the identification of malware and, this way, reduce phishing.

The **quarterly issue of this Security Newsletter** is one of the ways used to inform and alert on safety issues.

However, the following are always available at www.millenniumbcp.pt:

- The **Security area** fully dedicated to this issue which you may consult by going to "M - All about: Security".
- Whenever we identify a new phishing method, we place a warning in the website's homepage describing the method used. These articles have, whenever possible, images of the forged web pages or the contents of the fraudulent e-mail. The **Security Notices** are available at the Security area (M tab > All about Security > Security Notices).
- This web page contains **recommendations for using the channels securely**, as per the example provided below:

Access accounts



Security Tips

We **NEVER** ask you for a phone number or to install software to access online banking. →

and

Please never enter the whole number of your Multichannel Access Code. In case it is requested, please contact 707 50 24 24.

- After login, and **if left unused for a few minutes, the session will expire**. Notwithstanding this automatic security mechanism, always close your session using the respective option, "Logout", available on the upper right-hand corner.

- After accessing the website, you will get **information on the previous login**, date, time and channel. This way, you will be able to confirm logins made by you and warn the bank whenever you detect suspicious situations.

My Page

Welcome,

Last log-in: 27/06/2017 17:11:56 Mobile - Apps (SM-G935F)

✉ BancoMail ⌚ Pending Operations

ℹ Keep your personal data always updated.

User since 2001 Client since 1997

(access to the Individuals website)

Welcome to Online Banking

Welcome,

Last log-in: 2017/06/26 17:52:21

✉ BancoMail see 0 New Messages

ℹ **Aviso de segurança:** Alerta para mensagens fraudulentas.

@millenniumbcp.pt

(access to the Corporate website)

- The option **Operations History** makes it easier and quicker to view transactions carried out online with your access codes.

M Area Transfers

Services

Finance Manager

Transactions History

Unlock App Millennium

PUK APP Millennium

Security

(access to the Individuals website)

Iberian Offer

File Management

Authorizations Pending Transactions

Other Services Authorisation Rules

Transaction History

Providers & Others Scheduled Events

(access to the Corporate website)

- The **Alerts** service enables the user to receive an e-mail (free) or text message (subject to pricing) alerts regarding debit or credit entries to the current deposit accounts or charges to credit cards.

You may create your Alerts using the following options:



(access to the Individuals website)

Other Services

Alerts

- › Balances
- › SEPA Direct Debits
- › Payments and Transfers
- › Cards
- › Cheques
- › Trade Finance
- › Anomalies in Processing

(access to the Corporate website)

We also inform that, for safety reasons:

- Millennium bcp never sends links in e-mail messages;
- Millennium bcp's homebanking NEVER request the mobile phone number or the installation of security software. The pop-up bellow is displayed in the most recent phishing attack, do not provide any data and contact us immediately:



If you ever find something out of place at www.millenniumbcp.pt or if you need further information please call us on 707 50 24 24 (Personal Assistance 24/7).

Source: Millennium bcp

REMEMBER...



If you are on holidays, travelling, at the coffee shop or even at the beach, it is likely that, through your laptop, smartphone or tablet you will want to make sure you are online.

Currently, access to public Wi-Fi is available everywhere through hotspots.

A public hotspot is a wireless network configured to provide shared internet access. The hotspot provider buys an access point, connects it to the internet and transmits the signal in a public area, enabling anyone with a device that is within reach to access the network and go online for free.

Since the responsibility for the use of public hotspots falls entirely to the user, here are some suggestions:

- Please take into attention your surroundings. By definition, public Wi-Fi networks are not safe;
- Do not allow your mobile device to automatically connect to the nearest network. Manually choose the hotspot when you wish to go online;
- Never make purchases or bank transactions when using a public hotspot;
- Only use e-mails and messages for casual conversations. Create a separate e-mail account to use when online through public hotspots;
- Disconnect your device's Mobile Data when not in use;
- Never use the same access code on different websites. You may unknowingly give access to your various accounts;
- Make sure you have software designed to protect you from viruses, malware, trojans or other malicious programmes and make sure you update it regularly;
- Update your operating system and anti-virus software regularly.
- Public hotspots may be useful while travelling, provided that you take precautions.

Remember that you are responsible for protecting your device, your data and your privacy with good tools and for using them securely!

Source: Millennium bcp

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.

