NEWSLETTER SEGURANÇA

Millennium bcp Prestige

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:

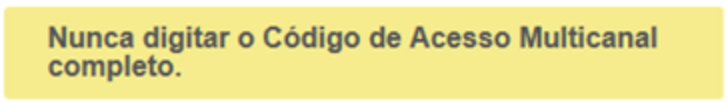
- A **área de Segurança** totalmente dedicada a este tema, que pode consultar acedendo ao menu "M > Tudo sobre > Segurança".

- 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).

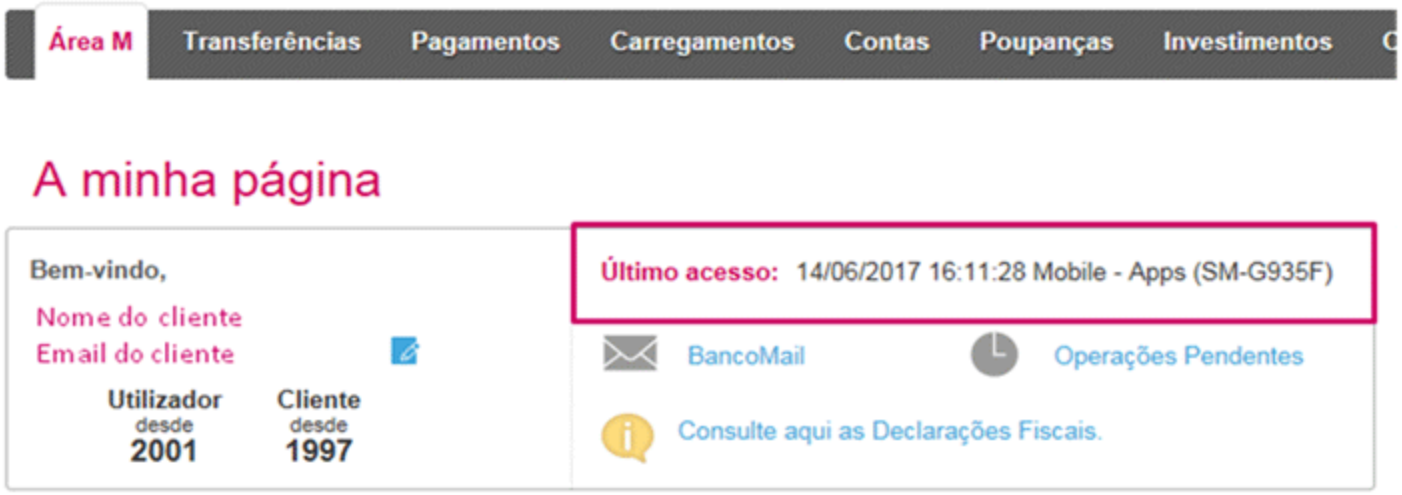
- Na página de acesso existem **recomendações para uma utilização segura**, conforme exemplo abaixo:

e

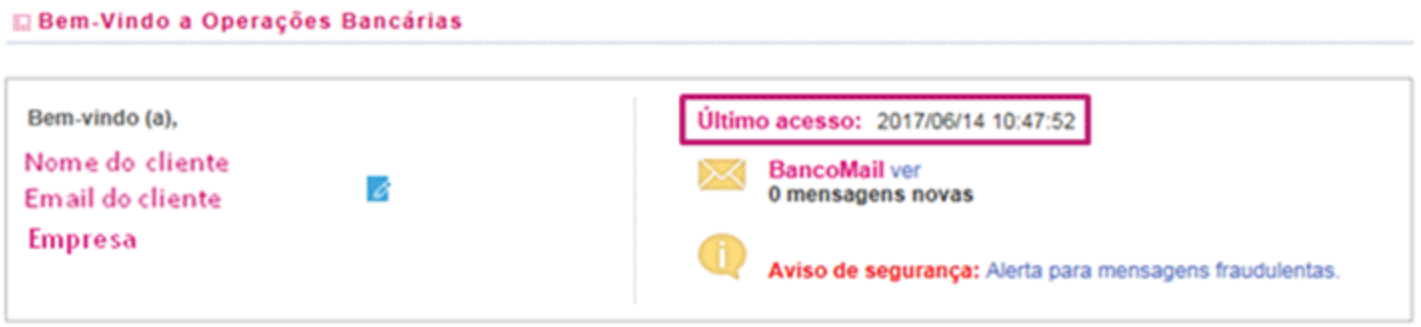


- Após login, e **ao fim de alguns minutos de inatividade, a sessão expira.** Não obstante existir este automatismo de segurança, termine sempre a sua sessão, na opção respetiva, "Terminar sessão", no canto superior direito.

- 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.



(acesso à área de Particulares)



(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.

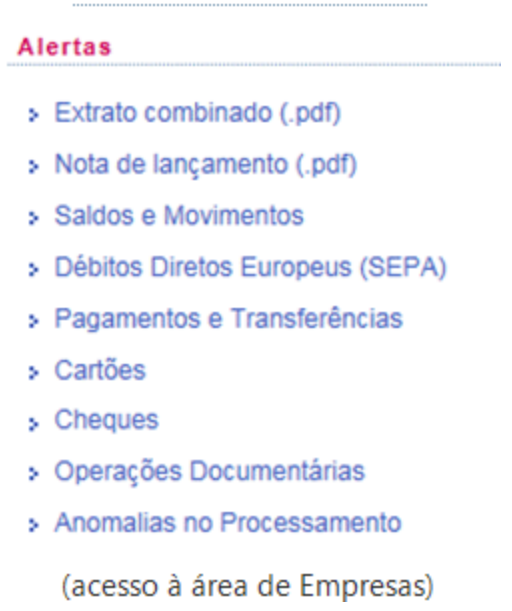
(acesso à área de Particulares)

(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)



(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:

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

Versão portuguesa

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.

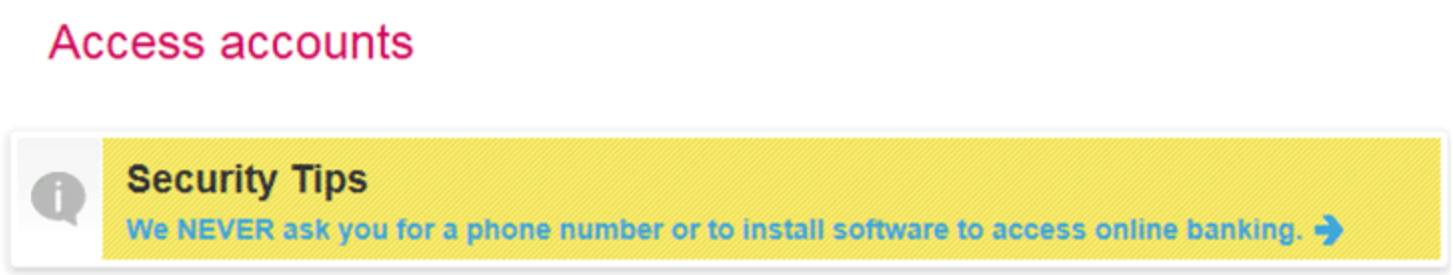
The **quarterly issue of this Security Newsletter** is one of the ways used to inform and alert on safety issues.

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:

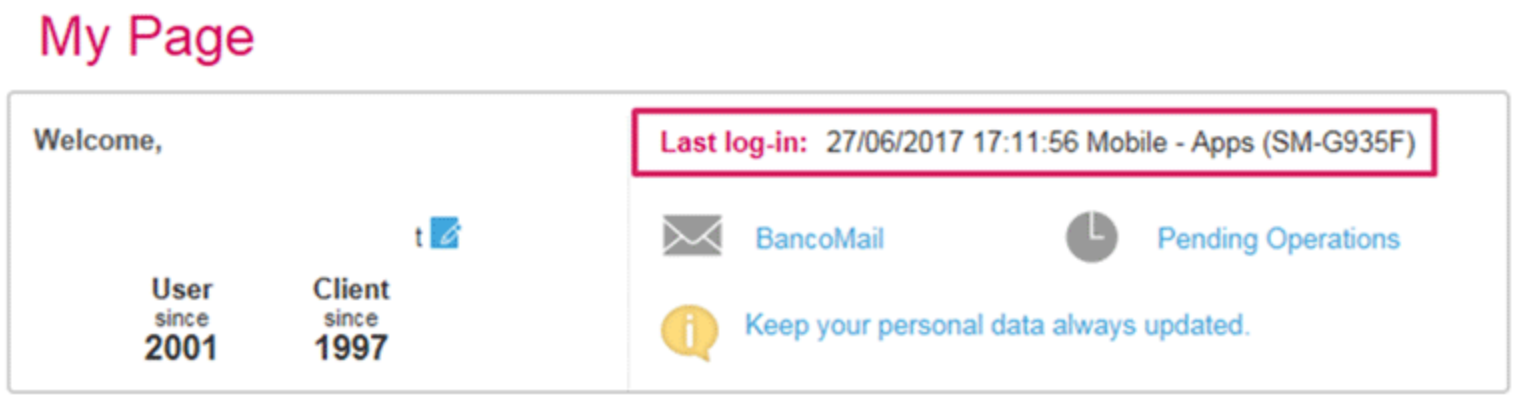


and

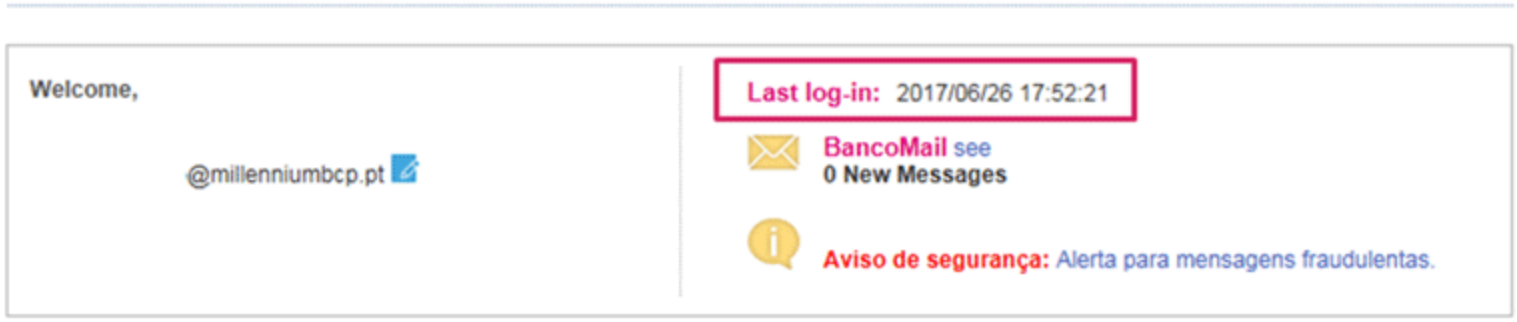
Please never enter the whole number of your Multichannel Access Code. In case it is requested, please contact 707 50 24 24.

- 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.

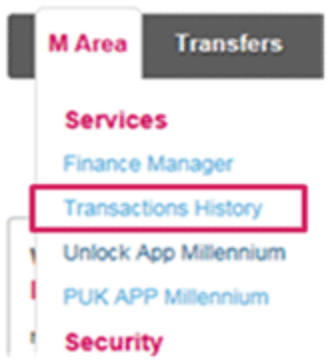


(access to the Individuals website)

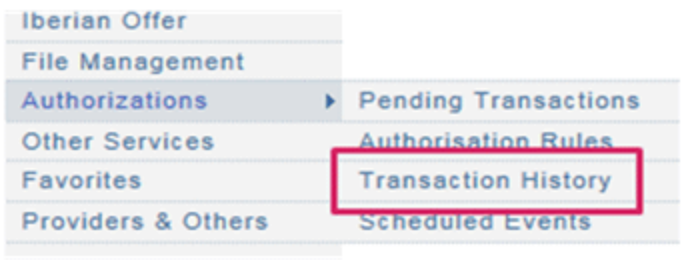


(access to the Corporate website)

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



(access to the Individuals website)

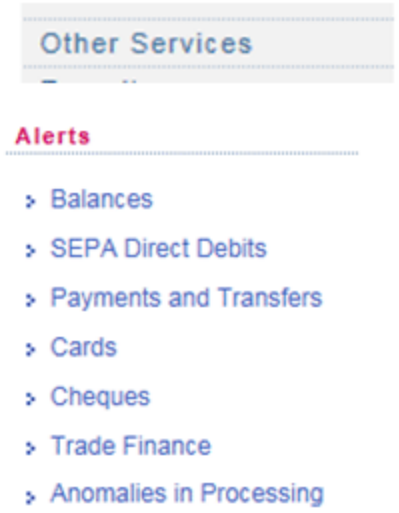


(access to the Corporate website)

- 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)



(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