NEWSLETTER SEGURANÇA

Millennium bcp

AGOSTO 2016 Nº 76

English version

Cada vez mais os *smartphones* são objetos pessoais e intransmissíveis.

Atualmente, estes equipamentos contêm uma série de informação pessoal/privada, bem como, permitem o acesso direto a algumas aplicações (app's) sem necessidade de autenticação *(password's).*

Contactos pessoais, SMS's, notas, recados pessoais, caixas de correio eletrónico e redes sociais com acesso direto, bem como, os registos pessoais (fotos, vídeos, etc) são alguns dos dados que, caindo em mãos erradas, podem ser prejudiciais para si e para os seus contactos.

Para evitar situações desagradáveis, defina uma *password* para acesso ao equipamento. Proceda, igualmente, à ativação do sistema de bloqueio automático quando o equipamento fica inativo por um período de tempo. Faça regularmente um *backup* dos seus dados para que tenha sempre uma cópia atualizada.

Sabe que existem App's de alarme anti roubo?
Este tipo de aplicações podem fazer o equipamento vibrar, emitir sinais sonoros e luminosos alertando para o facto de alguém estar a experimentar *passwords* aleatórias para aceder ao *smartphone.* Estes aplicativos também podem permitir que defina um alarme caso movam ou desloquem o equipamento, o qual irá atrair a atenção de todos em redor.

Outro cuidado que deve considerar é **o acesso por redes *Wi-Fi* gratuitas,** disponibilizadas em locais públicos. Sem dúvida, são muito convenientes mas… **pouco seguras!**

Para aceder a uma rede *Wi-Fi* gratuita, não é necessário efetuar qualquer tipo de autenticação ou a *password* está disponível num local visível, o que facilita o acesso à rede e também o trabalho dos cibercriminosos, que intercetam os dados pessoais (ex: *passwords)* colocando-se numa posição intermédia entre o equipamento móvel e o ponto de acesso *(man-in-the-middle).* Ou seja,

em vez de o equipamento móvel estar ligado diretamente ao ponto de acesso, está a comunicar com o cibercriminoso que regista a informação e retransmite para o ponto de acesso.

Através desta ligação gratuita evite aceder a quaisquer *sites* que requeiram a introdução de informações sensíveis, incluindo redes sociais, compras *online* e *homebanking.* Neste tipo de acessos utilize sempre a rede de dados do seu equipamento móvel.

Outra ameaça que deve considerar no caso do roubo de dados é o *software* malicioso que pode ser instalado no seu equipamento por via de SMS, e-mail, aplicações não oficiais, de entre outras.

Para os cibercriminosos, estas são formas rápidas de se apoderarem dos equipamentos móveis e roubar dados pessoais/privados.

Proteja-se e proteja o seu *smartphone/tablet* com uma aplicação de antivírus, efetuando as atualizações periódicas indicadas pelo fornecedor. Existem aplicações gratuitas nas *stores* oficiais.

Tenha, também, muito cuidado se por contacto telefónico, SMS ou por e-mail lhe sejam solicitados os seus dados pessoais. **Pode não se tratar de um esquema malicioso, mas sim uma forma de angariar os seus contactos para campanhas de SPAM.**

Considere desativar o *Bluetooth* quando não precisar. O seu telemóvel ficará menos vulnerável e ciberataques e consumirá menos bateria.

Adicione a sua informação enquanto proprietário do *smartphone.* A maioria dos equipamentos permite disponibilizar informação do proprietário no écran inicial mesmo que este esteja bloqueado. Se o perder, e caso alguém sério o encontre e o queira devolver, tem informações para o poder contactar.

Finalmente... Mantenha o *smartphone* seguro fisicamente.

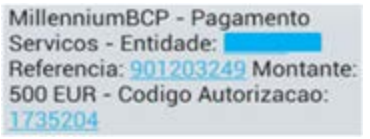
Cada vez mais o telemóvel é um objeto pessoal, contém informação sensível, pelo que, mantenha-o sempre perto de si!

LEMBRE-SE QUE...

- O Millennium bcp não envia mensagens de correio eletrónico ou SMS com *links* e nunca solicita elementos de caráter pessoal e/ou confidencial aos seus Clientes;
- Nunca faculte a terceiros os Códigos de Autorização recebidos por SMS ou obtidos via Token, bem como, leia atentamente todo o conteúdo dos SMS's recebidos com Códigos de Autorização, os quais identificam os dados da operação que registou, por exemplo:

Transferência pontual
no valor de 127,43€

Transferência Western Union
para a Nigéria, no valor de 250€

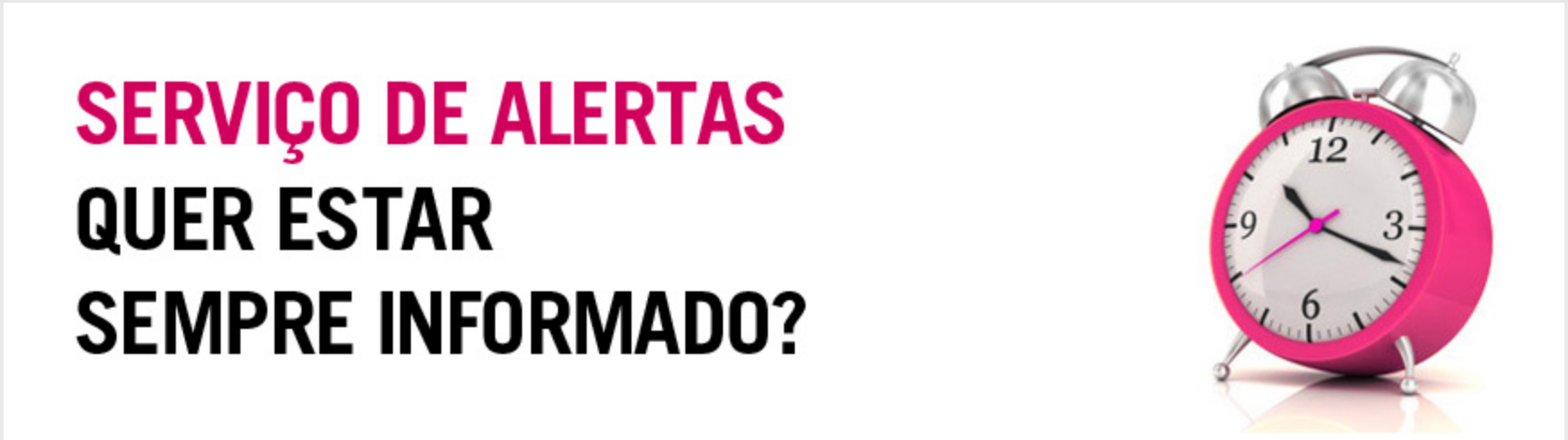


Pagamento de Serviços para a Entidade
xxxxx,
com a referência 901203249, no valor de 500€

- Os Códigos de Acesso ao Millennium bcp são pessoais e intransmissíveis pelo que sempre que suspeite que estes possam estar comprometidos, não hesite em alterá-los ou pedir o bloqueio através do serviço de atendimento telefónico ou de uma Sucursal Millennium bcp.
- Por questões de segurança, os canais Mobile do Millennium bcp incluem tempos limite de sessão e terminam automaticamente se estiver inativo após um período de tempo.

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

Fonte: Millennium bcp



Versão portuguesa

Smartphones are ever more personal and non-transferable devices.

Presently, these devices have lots of personal/private information, as well as allow the use of some apps without authentication required (password).

Personal contacts, SMSs, notes, personal messages, e-mail accounts and social networks with direct access, as well as personal records (photos, videos, etc) are some of the data that, in the wrong hands, could harm you and your contacts.

To avoid unpleasant situations set a password to unlock the smartphone. We recommend that you activate the automated lock screen after the device is inactive for a certain period of time. Regularly back up your data so that you always have an up-to-date copy.

Did you know that there are anti-theft alarm Apps?
This type of applications can make your smartphone vibrate, ring and light up when someone is trying out random passwords to unlock your smartphone. These apps also allow you to define an alarm should someone move or unlock the device, which will attract everybody's attention.

You should also be careful when accessing free Wi-Fi networks, available in public places. They are undoubtedly very convenient but also... **very unsafe!**

To use a free Wi-Fi network, it is not necessary to authenticate the user or the password is readily available, making it easily accessible and making the cyber-criminals' job easier when trying to access personal data (ex.: passwords), using the technique of getting in between the mobile device and the access point (man in the middle). I.e., instead of the device being directly connected to the access point, it is communicating with the cyber-criminal which records the information and reroutes it to the access point.

Avoid opening any website that requires sensitive information, including social networks, online shopping or banking, using free Wi-Fi connections. For these accesses, always use the network provided by your mobile operator.

Another threat you should consider in terms of data theft is malware that can be installed on your device via SMS, e-mail, unofficial apps, among others.

For cyber-criminals, this is one of the quickest ways to get into mobile devices and steal personal/private data.

You should protect yourself and protect your smartphone/tablet **with anti-virus software,** without forgetting to update it according to the seller's instructions. The official stores have free apps.

Also beware of phone calls, text or e-mail messages asking for personal data. **It may not be malware, but a way to get your contacts for spam mail.**

You should consider turning Bluetooth off when not being used. Your mobile phone will be less vulnerable to cyber attacks and it saves battery.

Add your information as owner of the smartphone. Most devices enable showing the owner info on the home or lock screen. That way, if you lose it and well-intentioned strangers find it, they will be able to contact you.

Finally... Keep your smartphone safe physically.

A mobile phone is ever more a personal object, with sensitive information, so keep it close to you!

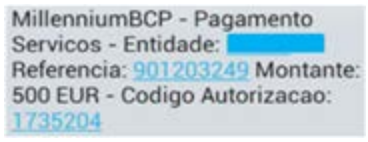
Source: Millennium bcp

REMEMBER...

- Millennium bcp never sends its customers e-mail or text messages with links or asking for personal or confidential information;
- You should never provide the Authorisation Codes received via SMS or Token to third parties, and you should carefully read the contents of the SMSs with the authorisation codes identifying the data of the operation you requested, for instance:

One-off transfer amounting to 127.43€

Western Union Transfer to Nigeria, amounting to 250€



Payment of Services to Entity xxxxx, reference 901203249, amounting to 500€

- Access codes for Millennium bcp are personal and not transferable, therefore should you suspect that they have been compromised, please change them as soon as possible or request that they be blocked using the phone channel or at a Millennium bcp branch.
- For security reasons, Millennium bcp's Mobile channels include limited time for a session and close automatically if inactive after a period of time.

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

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 @ 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”.

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