NEWSLETTER
SEGURANÇA

Millennium bcp

AGOSTO 2015 Nº 72

English version

Em período de férias é frequente recorremos mais ao *smartphone* ou ao *tablet*, contudo, em algum momento, já pensou:

- Que existem ataques direcionados também aos aplicativos *mobile*?
- Se os aplicativos instalados no seu *smartphone/tablet* estão a registar o que faz? As suas deslocações? As suas mensagens?
- Se o seu *smartphone/tablet* terá vírus? Instalou algum programa antivírus? Está atualizado?
- Que os seus dados pessoais, fotografias ou outra informação pessoal/confidencial guardada no seu *smartphone/tablet* podem não estar seguros?

Ainda existem muitos utilizadores que acreditam que os vírus, os ataques informáticos e outros problemas de segurança ocorrem apenas em computadores, esquecendo que os *smartphones* e *tablets* estão cada vez mais horas ligados à *Internet* e, consequentemente, mais expostos a riscos.

À semelhança do que acontece com os computadores, quanto mais utilizamos este tipo de equipamentos, novas ameaças e vulnerabilidades surgirão e maior será o número de vítimas de ciberataques.

Atualmente, existem vários aplicativos bancários para dispositivos móveis, pelo que, o acesso a contas, saldos, extratos, pagamentos, transferências, investimentos, etc., está

6) SMS desconhecido
Uma maneira comum de espalhar vírus é através de SMS. **Nunca** clique em *links* enviados por SMS de um contacto desconhecido, eliminando a mensagem e bloqueando o remetente, ou, caso seja de uma entidade fidedigna, sugerimos que confirme a veracidade do conteúdo contactando a entidade em causa, antes de aceder ao *link*. Neste caso, repetimos os conselhos acima indicados sobre os cuidados a ter antes de aceder a um *link*. Tenha também cuidado se o SMS lhe pedir uma resposta com os seus dados pessoais. **Pode não se tratar de *software* malicioso, mas sim uma forma de angariar os seus contactos para campanhas de SPAM.**

7) Redes não seguras
As redes *Wi-Fi* gratuitas disponibilizadas em locais públicos facilitam o acesso à *internet*, contudo, não são considerados acessos seguros. Habitualmente, para aceder a uma rede *Wi-Fi* gratuita, não é necessário efetuar qualquer tipo de autenticação ou a *password* está disponível num local visível, facilitando o acesso à rede e também o trabalho dos cibercriminosos que, para intercetar dados pessoais (ex: *passwords*), recorrem á técnica de se colocarem 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 com o ponto de acesso, está a comunicar com o cibercriminoso que regista a informação e retransmite para o ponto de acesso. **Evite**

ao alcance de todos, incluindo, dos cibercriminosos.

Esta é a nova realidade!

As principais apostas do Millennium bcp são a prevenção e a resposta rápida a situações como:

- Transações fraudulentas;
- Mitigação de riscos relacionados com o roubo de identidade e dados bancários.

Consequentemente, aumentamos a nossa preocupação com a arquitetura, desenho, implementação e configuração dos requisitos de segurança em aplicativos móveis.

Contudo, não nos podemos esquecer que o objetivo dos cibercriminosos é contornar os sistemas de segurança pelo que é necessário sensibilizar, criar hábitos e adotar regras na utilização dos equipamentos com ligação à internet, uma vez que a segurança depende do envolvimento de todos (utilizadores e entidades)!

Também precisa estar alerta a outras ameaças, como por exemplo:

1) Roubo
Os *smartphones/tablets* são equipamentos apelativos e, como tal, alvos de furto ou roubo. Defina uma *password* que limite o acesso de terceiros ao equipamento. Considere ativar o sistema de bloqueio automático quando o equipamento fica inativo por um período de tempo. Certifique-se, também, de fazer regularmente um *backup* dos seus dados para que tenha sempre uma cópia atualizada.

2) Vírus
Para os cibercriminosos, esta é uma das formas mais 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.

3) Aplicativos não oficiais
Aplicativos não oficiais são pontos de acesso para cibercriminosos. Deve recorrer sempre aos sites/*stores* oficiais quando necessitar de instalar uma aplicação. Antes de efetuar o *download* de uma aplicação, leia a opinião de outros utilizadores e verifique a que funcionalidades terá acesso no seu equipamento (ex: leitura e envio de sms, localização).

4) Manipulação de *e-mail*
Ao usar o *e-mail* no seu equipamento móvel, certifique-se de **nunca aceder a mensagens que não reconheça, principalmente a anexos ou *links***. No caso de receber algum *link* que o faça desconfiar, pergunte ao remetente utilizando outro canal, do que se trata e se é de confiança. Deve, igualmente, evitar o envio de informações confidenciais por *e-mail*.

5) Ameaças nas compras/vendas *online*
Os *sites* de compras/vendas *online* que guardam informações de dados pessoais e números de cartão de crédito/débito também sofrem ciberataques. **Utilize sempre uma rede 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.**

8) Armazenamento de dados não seguro
Proteger os dados dos *smartphones/tablets* é fundamental para garantir a sua privacidade. Se o equipamento móvel for roubado ou emprestado a amigos ou família, é necessário que tome medidas de proteção contra roubo ou perda. Faça um *backup* regularmente num cartão SD ou drive USB externo.

9) Ameaças de dados de localização
Os equipamentos móveis contêm informações de localização geográfica, que podem expor o utilizador a ameaças à segurança física. Para se proteger, **só ative** os serviços de localização via GPS e/ou *Wi-Fi* quando tiver necessidade de utilizar os mesmos (ex:. aplicação de navegação automóvel, registo de treinos de *running*).

Para minimizar o risco de um ciberataque mantenha o seu equipamento móvel com a versão mais recente do *software*, seja o sistema operativo, sejam as aplicações que utiliza. Com efeito, estas atualizações, entre outras vantagens, resolvem problemas e corrigem erros de segurança.

Porque a segurança é uma das prioridades do Millennium bcp, cumpre-nos alertar ativa e preventivamente os nossos Clientes para situações de fraude/phishing as quais podem ser consultadas em millenniumbcp.pt, menu M - Tudo sobre: Segurança e, na página seguinte, aceda a "Avisos de Segurança".

Aproveitamos a oportunidade para relembrar que:

- O Millennium bcp **não envia** mensagens de correio eletrónico com *links*;
- **Nunca aceda** ao *site* do Millennium bcp **através de *links*** de mensagens, motores de pesquisa ou, mesmo, através da opção "Favoritos". Digite sempre o endereço completo www. millenniumbcp. pt;
- Por questões de segurança, o seu Código de Utilizador **só pode ser usado num equipamento móvel**, pelo que se pretende instalar a App Millennium num segundo equipamento é necessário criar um novo Código de Utilizador. Na recente versão da App em IOS no momento da instalação é criado automaticamente um novo código de utilizador;
- Atingindo as três falhas consecutivas de PIN, a App Millennium só pode ser desbloqueada através da introdução de um **código PUK** o qual está disponível para consulta em millenniumbcp.pt, após login, menu Área M, Consultar PUK APP;
- **Caso precise de reinstalar a App Millennium**, por exemplo, por atualização do sistema operativo do *smartphome/tablet* é necessário que proceda ao "Desbloqueio da App Millennium", operação disponível no site Millennium bcp e, após login, menu Área M. Na recente versão da App em IOS já não é necessário este procedimento;
- **Leia atentamente** o conteúdo dos SMS's recebidos com Códigos de Autorização, uma vez que os dados da

segura para aceder e efetuar compras nestes *sites*, **através de um equipamento móvel, e faça *logout* no final da compra**. Use serviços como o MBNet (cria um número de cartão de crédito virtual) ou Apps de bancos nacionais (permitem pagamentos de serviço, transferências). À semelhança da App Millennium outras aplicações bancárias incluem tempos limite de sessão e terminam automaticamente se estiver inativo após um período de tempo. Contudo, para estar seguro, **termine sempre as aplicações ativas no seu *smartphone/tablet*.**

- operação são identificados no texto do SMS;
- **Não deve fornecer quaisquer dados pessoais ou bancários por telefone** a supostas entidades que o contactem, sugerindo que desligue a chamada e contacte a entidade em causa, por forma a confirmar a veracidade desse contacto.

Fonte: Millennium bcp

LEMBRE-SE QUE...

Se verificar alguma situação anómala no site ou nas App's do Millennium bcp, por favor contacte-nos através do telefone 707 50 24 24 (Atendimento personalizado 24 horas).

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

Fonte: Millennium bcp

SERVIÇO DE ALERTAS
QUER ESTAR SEMPRE INFORMADO?

siga-nos no facebook

MOBILE

Esta informação é da responsabilidade do Millennium bcp.

Versão portuguesa

On holidays it is normal to use the smartphone or tablet more, yet have you considered:

- That there are also threats targeting mobile applications?
- That the applications installed on your smartphone/tablet could be tracking what you do? Where you go? Your text messages?
- That your smartphone/tablet could have a virus? Have you installed antivirus software? Is it up-to-date?
- That your personal information, photographs or other personal or confidential data saved on your smartphone/tablet could not be safe?

There are still many users who believe that viruses, computer hacking and other security issues only occur on computers, forgetting that smartphones and tablets are connected to the internet many more hours and therefore more exposed to risks.

Just like with computers, as we use this type of devices more and more, new threats and vulnerabilities will come and the number of victims of cyber-attacks will increase.

Nowadays, there are various banking applications for mobile phones, therefore access to accounts, statements, balances, payments, transfers, investments, etc. is at everyone's reach, including cyber-criminals.

This is the new reality!

6) Unknown text message (SMS)
A common way of spreading a virus is through an SMS. **Never** open links sent by text message by an unknown contact, delete the message and block the sender, or, if it was sent by a trustworthy entity, we suggest that you check whether the contents are true by contacting that entity before opening the link.
In this case, please read the advice provided above on how to be safe when opening links. Also beware of text messages asking for personal data. **It may not be malware, but a way to get your contacts for spam mail.**

7) Unsecure Networks
Free Wi-Fi networks available at public locations make going online easier but are not considered safe access spots. Usually 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. For these accesses, always use the network provided by your mobile operator.**

8) Unsecure data storage

Millennium bcp's main bet is on prevention and on acting fast to solve problems such as:

- Fraudulent transactions;
- Mitigating risks related to theft of identity and bank data.

Consequently, we increase our concern with the architecture, design, implementation and configuration of safety requirements on mobile devices.

Yet, one cannot forgo that the goal of cyber-criminals is to overcome security systems, therefore one must raise awareness, create habits and adopt rules for using devices with internet connection, since safety depends on everyone cooperating (users and banks)!

You should also be aware of other threats, such as:

1) Theft
Smartphones/tablets **are appealing devices and therefore targeted by thieves.** You should choose a password that limits access to the device by third parties. Please consider activating the auto-lock when the device is not used for a period of time. You should also regularly back up your data so that you always have an up-to-date copy.

2) Viruses
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.

3) Unofficial applications
Unofficial applications are access points for cyber-criminals. You should always use official websites/stores when you need to install an application. Before you download an app, read other customers' reviews and check what the app will need to access on your device (ex: reading and sending texts, location services).

4) E-mail
When using your e-mail account on your mobile, make sure you never **open e-mails you do not know, especially annexes or links**. If you receive a suspicious link, ask who sent you the link what it is and whether it is trustworthy using another communication channel. You should also avoid sending confidential information by e-mail.

5) Threats from online shopping/sales
Online shopping/sales websites that keep personal information and credit/debit card numbers are also the target of cyber-attacks. **Always use a secure network to open and use those websites, through a mobile device, and logout when you're finished.** Use services such as MBNet (creates a virtual credit card number) or the apps of domestic banks (allow payment of services, transfers, etc.). As happens with the Millennium App, the bank applications include limited time for a session and close automatically if inactive after a period of time. Yet, just to be safe, **always log out and close the active applications on your smartphone/tablet.**

Protecting the data on your smartphones/tablets is fundamental to ensure privacy. If your mobile device is stolen or lent to friends or family, it is necessary for you to adopt protection measures in case it gets lost or stolen. Regularly back it up onto an SD card or external USB drive.

9) Threats due to location services
Mobile devices provide location data that can compromise the user's physical security. To protect yourself, **only activate** the GPS and/or Wi-Fi location services when necessary (e.g. using GPS navigation when driving, logging running practices).

To minimize the risk of a cyber-attack, always keep your mobile device up to date, both the operating system and the applications. In effect, these updates, among other advantages, solve problems and correct security faults.

Because safety is one of the priorities of Millennium bcp, it is our duty to, in an active and preventive manner, alert our Customers for the fraud/phishing situations we are able to detect, which may be seen at millenniumbcp.pt, menu M - Everything you need to know on: Security and, on the next page, read the "Security Notices".

We also take advantage of this opportunity to remind you that:

- Millennium bcp **does not send** e-mail messages with links;
- You should **never open** Millennium bcp's website **through links** on messages, search engines or even through your "Favourites". Always type the complete address www. millenniumbcp. pt;
- For safety reasons, your User Code **can only be used on one mobile device**, therefore if you wish to install the Millennium App on a second device you need to create another User Code. The most recent version of the App for IOS automatically generates a new user code when it is installed;
- When the PIN code is wrong three times in a row, the Millennium App can only be unlocked using a **PUK code** that can be viewed at millenniumbcp.pt, after the login, menu M, View PUK APP;
- If you need to reinstall the Millennium App, for instance, due to an update of the smartphone/tablet's operating system, you must "Unlock the Millennium App", which is available in Millennium bcp site, after the login, on menu M. The most recent version of the App for IOS no longer requires this procedure;
- Please **read carefully** the SMS received containing the Authorisation Codes since the transaction data are identified in the SMS;
- **You should never provide personal or bank data by phone** to alleged entities that contact you and we suggest that you disconnect the call and contact the entity in question to verify the authenticity of the contact made.

Source: Millennium bcp

REMEMBER...

If you ever find something out of place at Millennium bcp site or Apps, please call us on 707 50 24 24 (Personal Assistance 24/7).

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.