



## Em destaque

Proteja-se de fraudes efectuadas através da Internet

Mais +



## Princípios básicos de segurança

Cuidados a ter com a utilização de produtos e serviços bancários

Mais +

[English version](#)



**NOVO**

**Panda Antivirus Pro 2009**  
protecção mais simples, rápida e intuitiva para o seu computador.  
Licença de 2 anos para 3 computadores.

© Panda Security 2008

Visite a área de Shopping em [www.millenniumbcp.pt](http://www.millenniumbcp.pt)!



## Em destaque

### Proteja-se de fraudes efectuadas através da Internet

No Millennium bcp a segurança é uma área a que dedicamos especial atenção. O propósito destes cuidados é garantir um sólido elo de confiança no relacionamento com os Clientes qualquer que seja o canal utilizado para aceder ao Banco.

Tendo em conta a crescente sofisticação das fraudes perpetradas através da Internet, e com o sentido de reforçar a confiança e de promover a utilização do [millenniumbcp.pt](http://millenniumbcp.pt), apresentamos de seguida um conjunto de recomendações relevantes para os Utilizadores da Internet:

#### Os seus códigos pessoais

Os códigos de acesso ao site do Millennium bcp e serviço de Mobile Banking são pessoais e intransmissíveis e não os deve dar a conhecer a ninguém, mesmo que solicitado por pessoas que se identifiquem como colaboradores do Banco.

Relembramos aqui alguns requisitos de segurança que deverão ser considerados para protecção da sua informação pessoal:

- Não partilhe os Códigos Pessoais. Se suspeitar que os seus Códigos são do conhecimento de terceiros, entre de imediato em contacto com o [millenniumbcp.pt](http://millenniumbcp.pt);
- Ao aceder a [millenniumbcp.pt](http://millenniumbcp.pt), introduza os Códigos Pessoais, apenas em zonas encriptadas do site. Esta zona é definida pela indicação <https://www.millenniumbcp.pt> na barra de endereço do browser, antes do nome da página que está a aceder, e pela existência de um "cadeado";

- Altere regularmente a password/multicanal e a chave de confirmação. Pode fazê-lo a qualquer momento em [www.millenniumbcp.pt](http://www.millenniumbcp.pt), área de Personalização, ou através do serviço de Banca Telefónica (para o código multicanal).

### **Anti-Vírus**

O acesso à Internet deverá ser sempre efectuado a partir de um computador com um programa anti-vírus instalado e actualizado, com as opções de protecção "Internet mail" e "downloads" activas. Trata-se de uma forma de proteger o seu computador contra *software* malicioso, como um *Trojan/Malware*, com capacidade para comprometer a segurança de um computador ou capturar e transmitir informação pessoal a terceiros.

### **E-mail**

É uma ferramenta de grande utilidade mas, se não forem tomados os cuidados necessários, pode transformar-se na chave que abre a porta do seu computador à utilização por pessoas mal intencionadas. Sempre que tiver dúvidas sobre a origem da mensagem ou sobre o conteúdo, por mais apelativo que seja o "assunto", deve apagá-la de imediato, sem a abrir, efectuar "forward" ou tomar qualquer outra acção sobre a mensagem; mesmo depois de ter analisado a mensagem com um programa anti-vírus.

### **Computadores partilhados**

Sempre que pretenda aceder a informação reservada, bancária ou não, através da Internet, utilize um computador cujo acesso e utilização esteja limitado a si ou a pessoas da sua confiança. O acesso a partir de computadores partilhados (por exemplo a partir de ciber-cafés ou de pontos de acesso colocados em locais públicos) expõe, com elevada probabilidade, a informação a que pretende aceder e os elementos utilizados para o acesso (códigos e passwords) a terceiros mal intencionados.

### **Sistema operativo e *Browser* Internet**

Utilize sempre *software* devidamente licenciado e efectue regularmente a actualização do sistema operativo e do *browser* (navegador), actualizações essas que, na generalidade dos casos, se podem efectuar a partir da Internet.

### **Firewall**

A instalação de uma *firewall* no computador permite reduzir o risco de acessos indesejados, nomeadamente a partir do exterior. Alguns sistemas operativos, como é o caso do Windows XP e Windows Vista, já trazem uma *firewall* incorporada. Caso o sistema que utiliza não incorpore essa segurança, recomenda-se a instalação de *software* adequado.

Fonte: [millenniumbcp.pt](http://millenniumbcp.pt)

[Topo](#) 



Princípios básicos de segurança

Cuidados a ter com a utilização de produtos e serviços bancários

O advento da Internet veio trazer um múltiplo leque de novas possibilidades em muitas áreas do nosso dia-a-dia.

No que diz respeito ao consumo de produtos e serviços bancários, não há dúvida que o acesso ficou francamente simplificado. Deixou de ser necessário deslocar-se à sua dependência bancária, passando a ser possível efectuar um grande número de operações bancárias, remotamente, através de um computador, PDA ou telefone de última geração. Consultar movimentos, efectuar transferências, pagar compras online, dar ordens de bolsa, são apenas algumas das hipóteses que estão ao alcance de qualquer utilizador de serviços bancários.

Mas, infelizmente, as oportunidades trazidas pelas novas tecnologias, não são apenas aproveitadas por pessoas de bem.

Por esse motivo, apresentamos alguns cuidados que consideramos necessários quando da utilização de produtos e serviços bancários:

- Tenha especial cuidado com a máquina que utiliza quando faz o acesso para o consumo dos produtos e serviços bancários. Evite ao máximo utilizar máquinas que não conhece, como por exemplo, computadores de quiosques.
- Não descarregue ilegalmente conteúdos (programas/jogos/filmes). Não apenas pela questão de estar em conformidade, mas porque este acto é potenciador de problemas futuros. Não raro o que se descarrega traz mais do que aparenta. Muitas vezes, o que é descarregado nas redes *peer-to-peer*(1) está infectado com vírus de difícil detecção. Vírus que pretendem tirar o máximo partido financeiro do ataque.
- Máquina com anti-vírus actualizado. Mesmo que não descarregue conteúdos da Internet, deverá ter a preocupação de ter o seu computador sempre com um programa de anti-vírus e de anti-spyware a funcionar e devidamente actualizado.
- A *firewall* do computador deve estar sempre ligada de modo a aumentar a segurança do mesmo.
- Cuidado por onde navega. Não navegue por sítios duvidosos porque, por muito boa protecção que tenha no PC, a prevenção é a melhor protecção de todas.
- Não partilhe credenciais com ninguém. Esta é uma regra de ouro que, infelizmente, nem sempre é tida em conta. Nunca se esqueça que em circunstância alguma deverá partilhar com terceiros, conhecidos ou desconhecidos, as suas credenciais, sejam elas quais forem. Se receber uma mensagem de correio electrónico em nome da sua instituição financeira a pedir as credenciais para validação, simplesmente apague essa mensagem. Se está a utilizar o acesso num sítio público (por exemplo, a partir do seu portátil) certifique-se que, na altura em que está a introduzir os dados, não está ninguém na proximidade a tomar atenção ao que está a escrever.

(1) Sistema que permite a um utilizador trocar e partilhar ficheiros com outros utilizadores de forma directa, ou seja, sem "intermediários".

Fonte: Microsoft



**Este e-mail é apenas informativo, por favor não responda para este endereço.** Para obter esclarecimentos adicionais, sobre este ou qualquer outro assunto, ou efectuar sugestões, e para que o possamos servir melhor e mais eficazmente, sugerimos que visite [www.millenniumbcp.pt](http://www.millenniumbcp.pt) ou ligue para o número de telefone 707 50 24 24.

**Estes e-mails não permitem o acesso directo ao site [www.millenniumbcp.pt](http://www.millenniumbcp.pt), 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 electrónico, aceda a [www.millenniumbcp.pt](http://www.millenniumbcp.pt) e escolha a opção Contas e, posteriormente, a opção Personalização.

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882

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

[www.millenniumbcp.pt](http://www.millenniumbcp.pt)

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24

## Security Newsletter

Millennium  
bcp

nº48

April 2009



### Highlights

Protect yourself against internet fraud

[More +](#)



### Basic security principles

Precautions to take when using online banking

[More +](#)

[Versão portuguesa](#)



Highlights

## Protect yourself against internet fraud

At Millennium bcp we take special care with security. Our aim is to ensure there is a solid bond of trust with our clients, regardless of the channel used to access the bank.

Keeping in mind the way internet fraud is becoming more and more sophisticated, and so as to bolster trust and promote the use of millenniumbcp.pt, here are some relevant tips for internet users:

### Your personal codes

The access codes to our site and Mobile Banking service are personal and non-transferable, and you mustn't pass them on to anyone, even if so requested by persons identifying themselves as bank employees.

Some security reminders to help you protect personal information:

- Don't show anyone your personal codes. If you suspect that others know your codes, contact millenniumbcp.pt immediately;
- When logging in to millenniumbcp.pt, enter your personal codes only in encrypted website pages. Encrypted pages will have <https://www.millenniumbcp.pt> before the name of the page you're accessing displayed on your browser's address bar, as well as a padlock icon;
- Change your password/multichannel and confirmation key often. You can do so at any time at [www.millenniumbcp.pt](http://www.millenniumbcp.pt)'s Customisation page, or by calling our Phone Banking service (for multichannel codes).

### Antivirus

You should always access the internet from a PC running updated antivirus software and turn on its 'Internet Mail' and 'Downloads' options. This way you'll be protecting your PC against malicious software, such as a trojans/malware, which have the capacity to compromise your PC's security, and find and send your personal information to others.

### Email

It is a very useful tool; however, if the necessary precautions aren't taken, it can turn into the key responsible for unlocking your PC to people with ill intent. Whenever you're in doubt as to the origin or content of an email message, no matter how appealing its subject is, delete it at once. Don't even open it, forward it or take any other action, even if you've scanned the message for viruses.

### Shared computers

When you need to access restricted information, banking or other, over the internet, use a computer that only you or people you trust use. Access from shared computers (e.g. cybercafés or public Wi-Fi access points) will greatly increase the risk of exposing your information, codes and passwords to malicious users.

### Operating system and internet browser

Always use licensed software and update your operating system and browser on a regular basis. You can nearly always run updates over the internet.

### Firewall

Setting up a firewall on your computer will reduce the risk of unwanted outside access. Certain operating systems, such as Windows XP and Windows Vista come with a built-in firewall. If the operating system you use doesn't come with this security feature installed, we highly recommend you install firewall software.

Source: millenniumbcp.pt

Top 



## Precautions to take when using online banking

The coming of the internet brought about a whole range of new possibilities that have changed our daily lives.

Access to banking products and services has certainly become much simpler. You no longer have to go to a bank branch and can carry out a great deal of banking operations remotely, over a PC, PDA or 3G mobile phone. Viewing transactions, making transfers, online shopping, stock exchange orders... these are only a few of the things a regular online banking user can do.

Unfortunately though, the opportunities these new technologies afford are also used by ill-intended people.

That's why we like to remind you of precautions you need to take when using online banking.

- Be wary of the computer you're using for your online banking. Avoid to the utmost using computers you don't know, such as computers at kiosks.
- Don't download illegal contents (software/games/movies); not only because it's illegal, but also because it can lead to future problems. What you download often contains more than meets the eye. A great number of times, peer-to-peer (1)downloads come infected with hard to detect viruses. Viruses that intend to take maximum financial advantage of the attack.
- An up-to-date antivirus. Even if you don't download contents from the internet, you should always keep your antivirus and anti-spyware software up-to-date and running.
- Your PC's firewall should always be active to ensure its security.
- Be wary of whereabouts you surf. Don't surf on dodgy sites: no matter how protected your PC is, prevention is the best protection of all.
- Don't share your details and passwords with anyone. This is a golden rule which, unfortunately, is often disregarded. Never forget that under any circumstance should you give any of your details to other people, whether you know them or not. If you happen to receive an email message on behalf of your bank requesting your details for validation, simply delete the message. If you're logging in say from your laptop in a public place, make sure that when you enter your details no-one is nearby watching what you are typing in.

(1) A network that lets users swap and share files directly, without mediation.

Source: Microsoft

Top 



***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 [www.millenniumbcp.pt](http://www.millenniumbcp.pt) or dial 707 50 24 24.

***These emails do not grant direct access to [www.millenniumbcp.pt](http://www.millenniumbcp.pt), nor do they include links\*, nor are they sent to ask for any personal details (namely access codes). If you do receive any such email, 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](mailto:informacoes.clientes@millenniumbcp.pt)***

*If you do not wish to receive such information via email or if you wish to change your email address, please go to [www.millenniumbcp.pt](http://www.millenniumbcp.pt) and click on Accounts, then Customize.*

*Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882*

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

[www.millenniumbcp.pt](http://www.millenniumbcp.pt)

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24