



## Em destaque

Nova área de Segurança do millenniumbcp.pt

Mais +



## Princípios básicos de segurança

Dicas para a segurança do PC durante as férias

Mais +

[English version](#)

Se os beneficiários das operações que frequentemente realiza são da sua confiança, porquê continuar a utilizar o Código de Autorização?

## Universo Financeiro Pessoal



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



## Em destaque

### Nova área de Segurança do millenniumbcp.pt

No Millennium bcp, damos uma grande importância à questão da Segurança. Nos dias que correm, a utilização da internet por indivíduos mal intencionados é cada vez maior, aumentando o número de fraudes efectuadas por esta via. Por esta razão, torna-se necessário uma especial e redobrada atenção nesta área.

Por isso decidimos, no millenniumbcp.pt, reformular a área de Segurança. Pretendemos reforçar um conjunto de recomendações que consideramos relevantes para todos os nossos Clientes utilizadores da Internet, assim como, garantir a confiança no relacionamento dos Clientes com o Banco através deste canal.

Introduzimos novos temas, podendo agora encontrar aqui toda a informação relevante sobre:

- Avisos de Segurança;
- A Segurança no serviço de Mobile Banking;
- **NOVO** Glossário de Segurança;
- Comprar com segurança (MBNet, Cartões, Cheques e SAFE – Sistema de Autenticação Forte electrónico).

### Avisos de Segurança

Toda a informação sobre emails suspeitos que estejam a ser enviados a Clientes, seja com vírus, sejam

acções de phishing com o objectivo de recolher informação das credenciais dos Clientes para uma eventual utilização maliciosa.

O Millennium bcp relembra que **nunca solicita elementos de carácter confidencial** por via de mensagens de correio electrónico e que as **mensagens de correio electrónico enviadas pelo Millennium bcp nunca contêm links nem qualquer software** para instalação imediata.

### **A Segurança no serviço de Mobile Banking**

O serviço de Mobile Banking permite a realização de operações com o máximo de segurança. Para isso, a cada utilizador do portal Millennium bcp, apenas será permitido o acesso ao serviço Mobile SMS a partir de um único número de telemóvel, indicado pelo Cliente aquando da activação do mesmo. Por outro lado, sempre que pretenda aceder às contas, cada utilizador terá de indicar o username e a password, tal como faz quando acede do seu PC ao portal Millennium bcp, e as operações bancárias, que não sejam consultas, necessitam de validação através da indicação de 3 dígitos da Chave de Confirmação.

Estas e outras informações sobre a Segurança do serviço de Mobile Banking podem ser consultadas a partir da página principal da área de Segurança do millenniumbcp.pt.

### **Recomendações de Segurança**

Como proteger o seu computador e a sua informação; como utilizar os códigos de acesso com critério e não se deixar iludir por acções de terceiros; como aceder ao Portal do Millennium bcp em segurança; como ensinar as crianças a melhorar a sua segurança na Web; estas são algumas das muitas recomendações de Segurança que poderá encontrar no millenniumbcp.pt. Temas actuais e de grande utilidade prática para todos os Clientes utilizadores da Internet e do serviço de homebanking.

### **NOVO Glossário de Segurança**

A introdução de um Glossário teve como objectivo explicar, de forma sucinta, os termos geralmente utilizados numa área de Segurança ligada à internet.

Agora, sempre que tiver dúvidas sobre um determinado termo desta área, pode pesquisá-lo no novo Glossário.

### **Comprar com Segurança**

Seja na Internet, com cartões de crédito ou através de cheques, temos que estar, nos dias que correm, atentos a possíveis fraudes.

Nesta área, pretendemos reforçar os aspectos a ter em conta para uma correcta e segura utilização dos meios de pagamento mais comuns, entre os quais se encontram as transacções efectuadas via Internet.

Consulte a nova área de Segurança em [www.millenniumbcp.pt](http://www.millenniumbcp.pt) > **Segurança**

The screenshot shows the Millennium BCP website interface. At the top, there's a navigation bar with 'Particulares', 'Empresas', 'Banca Investimento', and 'Institucional'. Below that, a secondary navigation bar includes 'Home', 'Contas', 'Segurança', 'Fundos', 'Bolsa', 'Cartões', 'Crédito', and 'Seguros'. The 'Segurança' menu item is circled in red, with a red arrow pointing to it from above. The main content area features a large banner with a target and a dart, advertising 'Na Earnings Season acerte no resultado e veja os Prémios'. To the right, there's a section for 'Mercados' with a table of stock indices. Below that, there's a 'Soluções' sidebar with various service categories like 'Acesso Contas', 'Particulares', 'Empresas', 'Mobile', and 'Sucursais'. A large red box on the right side of the page contains the text 'E você já tem o seu encosto?'.

Fonte: millenniumbcp.pt

Topo



## Princípios básicos de segurança

### Dicas para a segurança do PC durante as férias



Chegou o verão! Agora que as crianças terminaram a escola, muitos de nós começamos a preparar as férias. Porque o portátil é também utilizado como centro de diversão familiar e como forma de se estar contactável, é importante não esquecer a sua segurança. Abaixo encontra algumas dicas para o fazer.

#### Como tirar o melhor partido das redes públicas de WiFi

A esmagadora maioria dos portáteis mais recentes já tem incluída a capacidade de comunicar via redes sem fios, também conhecida como rede *wireless*. Com estas máquinas é possível ligar a redes *wireless* que já se

encontram disponibilizadas em múltiplos locais como aeroportos, restaurantes e hotéis. Para que esta facilidade não seja transformada em algo negativo, é preciso ter em conta alguns passos que ajudam a garantir a confidencialidade:

- **Utilize uma firewall.**

Se está a usar o Windows 7, Windows Vista ou Windows XP service pack 2 ou superior, o sistema operativo já tem uma firewall e, por omissão, já se encontra ligada. Certifique-se que a tem sempre ligada.

- **Não escreva números de cartão de crédito ou palavras-chave.**

Se utilizar uma rede *wireless* pública, idealmente não deverá escrever nem números de cartão de crédito nem palavras-chave, uma vez que estas redes são também utilizadas por hackers que

procuram constantemente vulnerabilidades para seu benefício pessoal. Mas, se tiver mesmo de utilizar palavras-chave e / ou números de cartão de crédito numa rede pública, deve ter em conta que o endereço Web deverá sempre começar com "https:" e não com "http:" e, no canto inferior direito do Internet Explorer, deverá encontrar um cadeado.

- **Se não necessitar da rede *wireless*, desligue-a!**

Esta é uma das fundamentais regras de segurança, se não necessitar de um determinado serviço, certifique-se que o mesmo está desligado. E é isso que deverá acontecer com a rede *wireless*. Tenha atenção que, por omissão, esta rede está ligada no seu computador.

### **Proteja a sua informação**

Se mantém informação pessoal e/ou financeira no computador, deverá investir num sistema operativo que permita a protecção ao nível do ficheiro. O Windows 7, Windows Vista ou Windows XP Professional incluem ferramentas que possibilitam a protecção da informação através de um processo chamado de encriptação.

### **Utilize palavra-chave forte**

Nunca é demais recordar o importante que é utilizar palavras-chave forte. O esquecimento desta regra facilita o acesso à informação que está no seu PC por qualquer pessoa mal intencionada. Uma palavra-chave forte terá de ter no mínimo 8 caracteres (idealmente 14 ou mais). Combine letras (maiúsculas e minúsculas), números e símbolos. Use palavras ou frases que sejam fáceis de recordar mas muito difíceis para outros adivinharem. Um exemplo de uma boa palavra-chave: "Feri@s! Finalm3nte!" (claro que, agora que está escrita publicamente, deixou de ser uma boa palavra-chave).



### **Faça cópias de segurança**

Especialmente quando o computador vai de viagem, a cópia de segurança deve ser efectuada. Deve ser feita antes de se iniciar a viagem, de preferência para um disco externo e não esquecer que o disco para onde se fez a cópia de segurança não deverá acompanhar o computador porque se assim for, em caso de perda / roubo do hardware, a informação também se perde. Durante as férias, especialmente antes do retorno, é uma boa ideia efectuar uma cópia das alterações efectuadas, para isso, poderá utilizar uma *pen drive* que provavelmente terá capacidade de guardar as fotos que tirou durante as férias.

### **Tenha especial cuidado com o que armazena nas *pen drives***

Com a crescente popularidade e aumento de capacidade aliados à baixa de preços, as *pen drives* fazem cada vez mais parte do nosso dia-a-dia. Perder uma *pen* representa um prejuízo bem maior do que o valor monetário da mesma. Porque é muito fácil perdê-la, tenha especial cuidado com a informação que aí deixa ficar. Evite ao máximo que informação de índole confidencial passe pela *pen* porque, mesmo que o ficheiro seja apagado, é possível recuperar a informação. Dica: para não perder facilmente a sua *pen drive*, coloque-a junto das chaves de casa / carro.

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

nº 49

July 2009



### Highlights

[millenniumbcp.pt's new Security page](#)

More +



### Basic security principles

[Summer holidays PC Security tips](#)

More +

[Versão portuguesa](#)




### Highlights

[millenniumbcp.pt's new Security page](#)

At Millennium bcp we attach a lot of importance to security. These days, there are more and more malicious users out there using the internet, and internet fraud hasn't stopped rising. There can be no room for carelessness here.

That's why we've decided, at millenniumbcp.pt, to make over our Security page. We'd like to remind you of some tips we believe the most important for clients using the internet and remind you that you can completely trust this channel for carrying out all your banking operations.

We've introduced new topics, and you can find all relevant information here regarding:

- Security Tips;
-  Security Glossary;
- Buy safely (MBNet, Cards, Cheques and SAFe - Strong Authentication System);
- Security Newsletters.

### **Security Tips**

How to protect your PC and data; how to safely access the Millennium bcp site; how to check the security certificate before inserting financial or personal data in a Web site; these are some of the many security tips you can find at millenniumbcp.pt. Current and useful topics for all those using the internet and our homebanking service.

### **Security Glossary**

This Glossary aims to explain, in a nutshell, the most commonly used terms in the context of security webpages.

Soon, whenever you're in doubt as to a given web-security term, you will be able to look it up in our new Glossary.

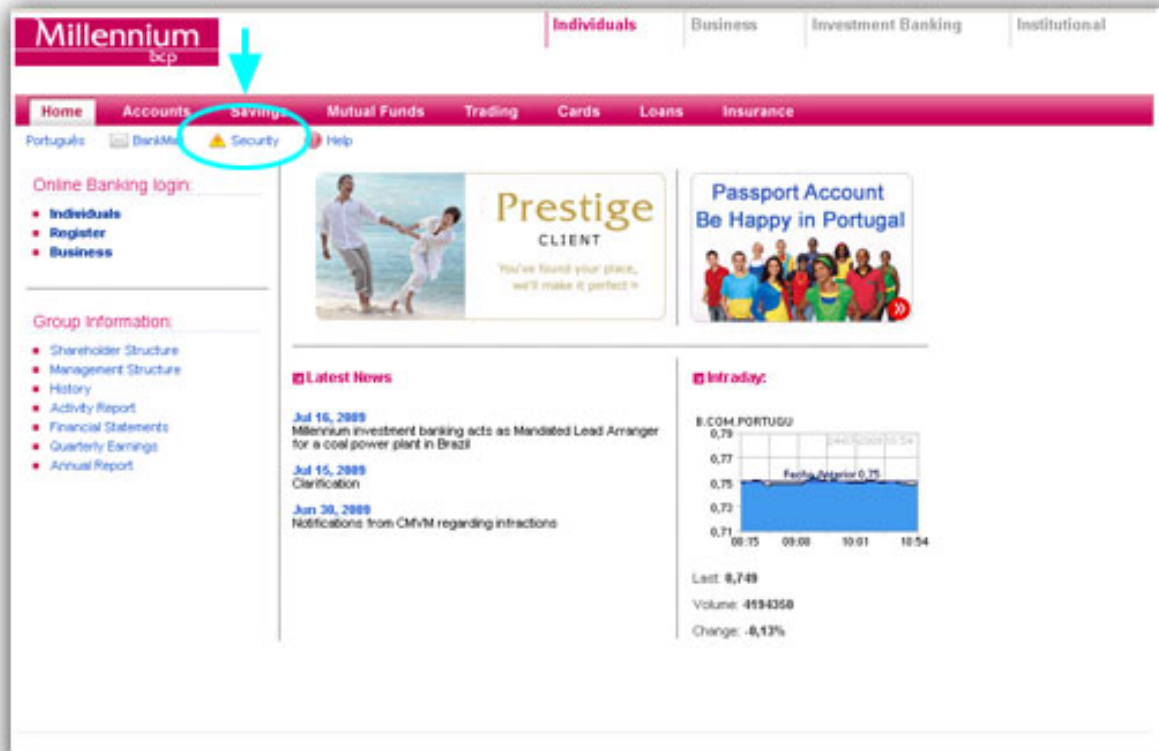
### **Buy safely**

These days, be it on the internet or with cheques, we must be on our toes and wary of potential fraud. On this page, we intend to go over some items you must keep in mind when using the most common means of payment safely and correctly, including over the internet.

### **Security Newsletters**

All the Security Newsletters that Millennium bcp has prepared in conjunction with Microsoft, with useful information for all those using the internet and millenniumbcp.pt.

Visit our new Security page at [www.millenniumbcp.pt](http://www.millenniumbcp.pt) > **Security**



Source: millenniumbcp.pt

Top 



## Basic security principles

### Summer holidays PC Security tips



Summer's here! Now that our kids are on summer break, many of us have started preparations to go on holiday. Since laptops are also used as for family entertainment and to stay reachable, it's important not to forget about its security. Here are some tips on how to keep your laptop secure:

#### How to best use public Wi-Fi networks

Just about all recent laptops have built-in wireless capacity. You can link up to wireless networks in a variety of places - airports, restaurants, hotels... To ensure this advantage doesn't turn sour, you should follow these steps to maintain confidentiality:

- **Use a firewall.**

If you're using Windows 7, Windows Vista or Windows XP service pack 2 or above, your operating system already comes with a firewall, which is turned on by default. Make sure you keep it on at all times.

- **Do not enter credit card numbers or passwords.**

If you use a public wireless network, then ideally you shouldn't type in such details since these networks are also visited by hackers, always on the lookout to use any vulnerability for their personal gain. However, if you really must enter passwords and/or credit card numbers on a public network, be sure that the web address has a "**https:**" and not a "http:" header, and that the bottom right corner of your browser displays a padlock icon.

- **If you don't need to use a wireless network, turn it off!**

This is a basic security rule - if you don't need a certain service, make sure it's turned off. So don't

forget to check the status of your wireless network. Keep in mind that it's on by default.

### Protect your information

If you keep personal and/or financial details on your PC, you should invest in an operating system that lets you protect your files. Windows 7, Windows Vista or Windows XP Professional include tools that let you protect your data by encryption.



### Use a strong password

It's never a waste of time to state the importance of using strong passwords. Forgetting this simple rule makes it easy for anyone to access the data on your PC. A strong password must have at least 8 characters (and ideally 14 or more). Combine letters (caps and lower case), numbers and symbols. Use words or phrases which you can easily remember but others will have a very hard time guessing. Here's an example of a good password: "Holid@ys!F1nally!" (of course, now it's been made public, it's no longer a good password!)

### Back up your files

Back up your data especially before taking your computer with you on holiday. You must back up your files before going on your holiday trip, preferably onto an external drive. Don't forget that you shouldn't take your backup drive along with your computer because if your equipment is lost or stolen, you'll also lose your files. It's always a good idea to make a backup copy before returning home of the changes you've made while on holiday. Use a pen drive (which will probably also be able to hold your summer photos).

### Be very careful with what you store on your pen drives.

With the rising popularity, increased storage capacity and low cost of pen drives, they're a growing part of our daily lives. Losing a pen drive is more than just losing the money you paid for it. And since it's so easy to lose, be especially careful as to the data you store on it. Avoid to the utmost leaving confidential details on your pen drive - remember that even if you delete a file, it's possible to recover the data that was on it. Tip: so as to make it harder for yourself to lose your pen drive, keep it with your house/car keys.

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.

