



Em destaque

Recomendações de segurança para pagamentos na Internet

[Mais ➔](#)



Princípios básicos de segurança

Postais eletrónicos fictícios

[Mais ➔](#)

[English version](#)



TOKEN READER

Códigos de autorização para confirmação das suas operações na internet, em Portugal ou no estrangeiro.

Visite a área de Shopping no site do Millennium bcp



Em destaque

Recomendações de segurança para pagamentos na Internet

A segurança dos pagamentos efetuados pela Internet é uma preocupação constante dos prestadores destes serviços e das entidades bancárias, que trabalham no sentido de estabelecer normas e procedimentos que garantam níveis de proteção elevados para os seus utilizadores e Clientes. O Millennium bcp não é exceção. Mas existe um outro fator determinante para o sucesso desta missão: a consciencialização e formação de segurança dos próprios utilizadores.

Nesta edição vamos apresentar-lhe informações importantes para que possa proteger as suas compras e pagamentos *online*, realizando-as com maior comodidade e segurança!

Assim, quando realizar as suas compras pela Internet, tenha em atenção as seguintes recomendações:

- A existência de um processo de registo onde lhe sejam atribuídas credenciais após a confirmação da aceitação das condições de utilização do *site*;
- Ferramentas e configurações necessárias para utilizar o *site*, por exemplo, antivírus, *firewalls*, versões mínimas de sistemas operativos e *browsers*, entre outros;
- Linhas orientadoras para a utilização mais correta do *site* e das suas credenciais, por exemplo, forma e frequência de alteração das credenciais, situações em que o acesso poderá ficar bloqueado e quais os procedimentos a adotar para o seu desbloqueio;
- Forma de funcionamento do *site* e da confirmação das transações, por exemplo, quais os passos para submeter e autorizar um pagamento;
- Quais os procedimentos caso necessite de participar a perda ou roubo das suas credenciais;
- Quais os procedimentos a adotar caso detete ou suspeite de uso abusivo das suas credenciais;
- Em que condições poderá suspender transações ou recusar a sua execução.

A segurança tem sido, desde sempre, uma das grandes preocupações do Banco e, como tal, o cumprimento das linhas orientadoras é para nós fundamental. O Millennium bcp tem trabalhado no sentido de consciencializar os seus Clientes para uma utilização correta e segura dos serviços de Banca Eletrónica e de garantir que os Clientes possam realizar as operações *online* com segurança, transmitindo informações pertinentes para a sua formação. Ficam aqui alguns exemplos do que temos neste momento implementado para a sua segurança:

- Contrato de Canais Remotos – a utilização dos canais Telefónico, Internet e Mobile obrigam à assinatura de um documento específico onde são apresentadas as condições gerais de utilização;
- Sistema de Autenticação Forte eletrónica (SAFe) – a confirmação de transações ou de informações mais sensíveis é sempre efetuada através de códigos únicos e de validade curta gerados via SMS ou Token;
- Disponibilização de Avisos de Segurança e Recomendações para acesso ao Site do Millennium bcp – através da área de Segurança do *site*, o Banco disponibiliza recomendações e informações importantes para uma utilização mais segura da página bem como avisos sobre as mais recentes ameaças conhecidas à segurança dos utilizadores;
- Newsletters de Segurança – disponibilizadas trimestralmente com informação sobre temas relacionados com a segurança *online* e formas de proteção da informação e dados pessoais;
- Comunicações Encriptadas SSL – todas as comunicações efetuadas entre os equipamentos do Cliente e o Banco (seja por computador ou equipamento móvel) são alvo de encriptação para garantir uma maior segurança da informação.

A proteção dos seus dados e informações depende muito de si!

Fonte: millenniumbcp.pt

Topo 



Princípios básicos de segurança

Postais eletrónicos fictícios

Os postais eletrónicos são criados do mesmo modo que os *websites*. Por isso, quando envia a alguém um postal eletrónico, envia-lhe um *link* onde clicar, que conduz ao postal de felicitações *online* que tiver criado. Isso significa que um postal eletrónico pode, na realidade, ser um esquema de *phishing*, *spam* ou um instalador de *spyware* ou de vírus informático.

Hoje deixamos aqui algumas dicas sobre como evitar postais eletrónicos falsos.

Comece por verificar sempre o nome apresentado e o endereço de correio eletrónico do remetente. Se não conhecer o remetente, não confie no postal. As empresas legítimas utilizam formas claras e padronizadas as quais lhe permitem reconhecer que a mensagem de correio eletrónico não é uma fraude. Por exemplo, com "MSN Greetings", o campo "De" indica sempre "Ecard from MSN Greetings" como nome apresentado e "ecards @ msn.americangreetings . com" como endereço de correio eletrónico.

Se não tiver a certeza sobre quem é o remetente ou qual a intenção da mensagem de correio eletrónico, não transfira ou clique em *links* de fontes desconhecidas, utilize métodos de visualização alternativos. Por exemplo, se utilizar o "MSN Greetings", poderá visualizar a felicitação no *website* do "MSN Greetings". Introduza "msn.americangreetings . com" no seu *browser* da Web e clique na ligação "ecard pickup" no canto superior direito.

Esteja atento a mensagens de correio eletrónico ou ficheiros anexos de remetentes que não conhece ou que lhe pareçam suspeitos.

Pré-visualize o endereço Web de um *link* antes de clicar no mesmo. Se não apresentar um endereço, desloque o ponteiro do rato sobre o *link*, sem clicar, para ver para onde está a direcionar (o endereço deve aparecer na barra inferior do seu *browser*).

Não aceite um acordo de utilizador final sem ler primeiro o texto em letras pequenas; poderá ser induzido a instalar *spyware* ou outros itens não desejados.

Utilize *sites* reputados de postais de felicitações quando enviar postais eletrónicos.

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 o site do Millennium bcp ou ligue para o número de telefone 707 50 24 24 (Atendimento Personalizado 24 horas).

Estes e-mails não permitem o acesso directo ao site do Millennium bcp, 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 site do 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.

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço electrónico, aceda ao site do Millennium bcp e escolha as opções: Contas, Personalização, Dados Pessoais, e posteriormente, Criar / Alterar endereço de e-mail.

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 3.000.000.000 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

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24
Atendimento personalizado 24 horas

Security Newsletter

Millennium
bcp

nº 59

July 2012



Highlights

Recommendations for the security of Internet Payments

[More](#) 



Basic security principles

Fake ecards

[More](#) 

[Versão portuguesa](#)



Highlights

Recommendations for the security of Internet Payments

The security of online payments is a constant concern of our services and of the banking entities that endeavour their best efforts to establish rules and procedures to ensure high protection levels for users and Customers. Millennium bcp is no exception. However, there is another factor that is crucial for the success of this mission: the security awareness and knowledge of the users.

In this edition we provide you with important information so that you may make secure online purchases and payments, all with the utmost security and comfort!

Thus, when you are shopping online, please take into consideration the following recommendations:

- The existence of a registration process where credentials are attributed to you after you confirm your acceptance of the website's terms and conditions;

- That you have the necessary tools and configurations to use the website, for example, antivirus, firewalls, minimum versions of operating systems and browsers, among other;
- The existence of guidelines on the best way to use the website and your credentials, for example, how and how often your credentials are altered, in which situations the access may be blocked and which are the procedures to adopt to unblock it;
- Information on how the website functions and how the transactions are confirmed, for example what you must do to submit and authorize a payment;
- Information on which procedures you must follow to report that your credentials were lost or stolen;
- Information on what can you do if you notice or suspect of an abusive use of your credentials;
- Information on how you can suspend or refuse the execution of transactions.

Security has always been one of the Bank's major concerns and, therefore, compliance with the guidelines is fundamental. Millennium bcp, by transmitting pertinent information to the customer, is continuously endeavouring to increase awareness on how to use Electronic Banking in a correct and safe manner, ensuring that customers are able to carry out online transactions safely. Please find hereunder some examples of some procedures we have implemented to increase safety:

- Remote Channels Contract – the use of the Phone, Internet and Mobile channels require a specific document signed by the Customer. This document presents all the utilization general conditions;
- Strong Authentication (SAFe) – the confirmation of transactions or of more sensitive information is always made through one short duration code generated via SMS or Token;
- Provision of Safety Warnings and Recommendations on how to access the Millennium bcp website – through the website's security area, the Bank provides important information and recommendations on how to use the website in a safer manner and notices on the most recent known threats to the user's safety;
- Security Newsletters – disclosed quarterly, these newsletters contain information on issues related to online security and ways to protect information and personal data;
- SSL Encrypted Communications – all communications made between the Customers' equipments and the Bank (by computer or by mobile) are encrypted in order to ensure increased data security.

You play an important role in the protection of your data and information!

Source: millenniumbcp.pt

[Top](#) 



Basic security principles

Fake ecards

Ecards are created the same way as websites. Therefore, when you send someone an ecard, you send them a link to click on and open the online greeting card you created. That means that an ecard may actually be a phishing scheme, spam, spyware or a virus executable.

Today we give you a few pointers on how to avoid fake ecards

Start by checking the sender's name and e-mail address.

If you don't know the sender, don't trust the card. Legitimate companies use clear and standard ways, easily recognisable, to convey that the ecard is not fake. For instance, with "MSN Greetings", "From" always displays "Ecard from MSN Greetings" as the name of the sender and "ecards @ msn.americangreetings . com" as the e-mail address.

If you are not sure who sent it or what's the intention of the e-mail, do not transfer or open links with unknown sources, using alternate means to view them. For example, if you are using "MSN Greetings", you may view the greetings at the MSN Greetings website. Go to "msn.americangreetings . com" and click on "ecard pickup" in the upper right corner.

Beware of e-mail messages or attachments with unknown or suspicious senders.

Preview the web address of a link before opening it. If it does not have an address, scroll the mouse pointer over the link, without clicking, to see what it links to (the address should appear on the lower bar of the browser).

You should not accept an end-user agreement without reading the fine print; you may be induced into installing spyware or other unwanted items.

Use well known greeting cards websites to send your ecards.

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 the Millennium bcp website or dial 707 50 24 24.

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 website 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 3.000.000.000 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

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24
24 hours Personalized Service