NEWSLETTER SEGURANÇA

Millennium bcp

MAIO 2016 Nº 75

English version

Alertas como “não partilhe os seus códigos de acesso”, “não aceda a *links* ou a ficheiros executáveis em mensagens de correio eletrónico suspeitas” e que “as instituições bancárias nunca enviam mensagens de correio eletrónico com *links*” são constantes, não sendo de estranhar que todas as instituições bancárias intensifiquem regularmente estes e outros alertas, nos respetivos sites, sobre mensagens de correio eletrónico não fidedignas, dando conselhos aos utilizadores de como evitar ser alvo de cibercrimes.

Afinal... a tecnologia está em constante evolução e os criminosos estão sempre a encontrar novas formas de a manipular.

Como utilizadores da internet devemos manter-nos sempre em vigilância e adotar regularmente novas medidas de segurança, sendo muito importante proteger os nossos dados pessoais, bem como, os equipamentos que usamos.

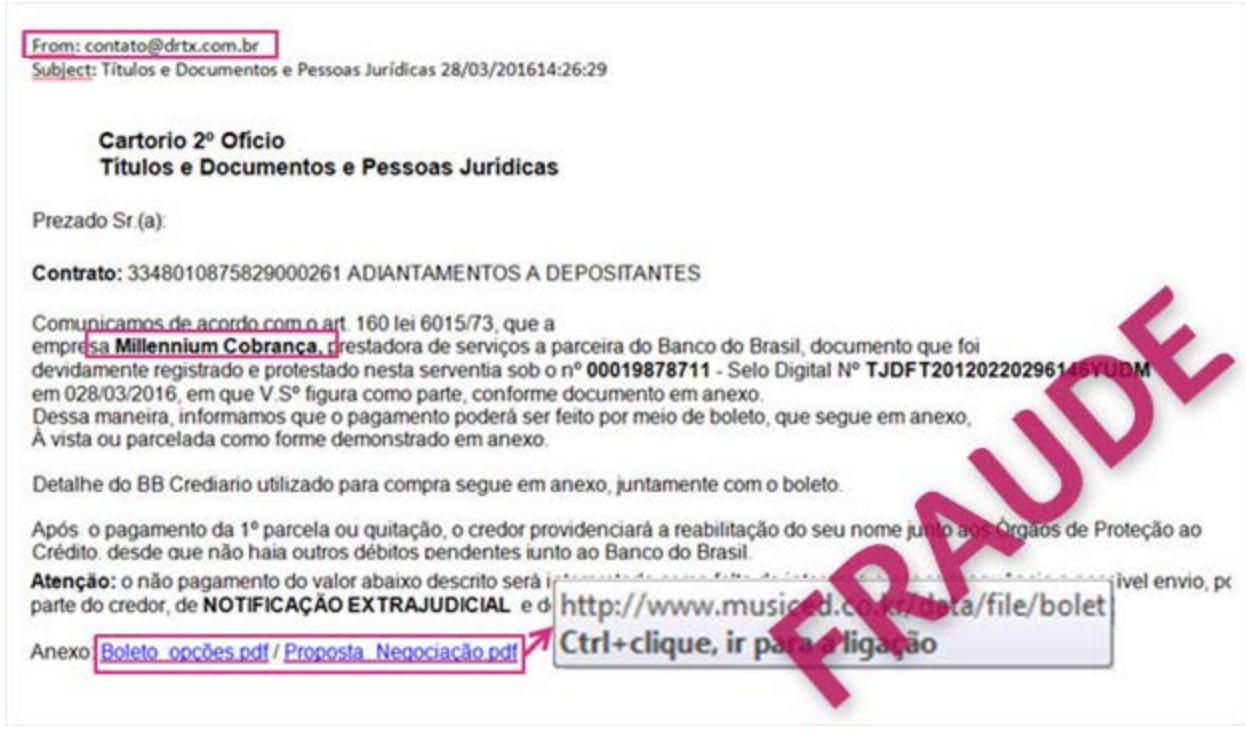
Assim sendo, deixamos algumas dicas sobre como manter a sua informação segura quando utiliza o Correio Eletrónico ou navega na internet:

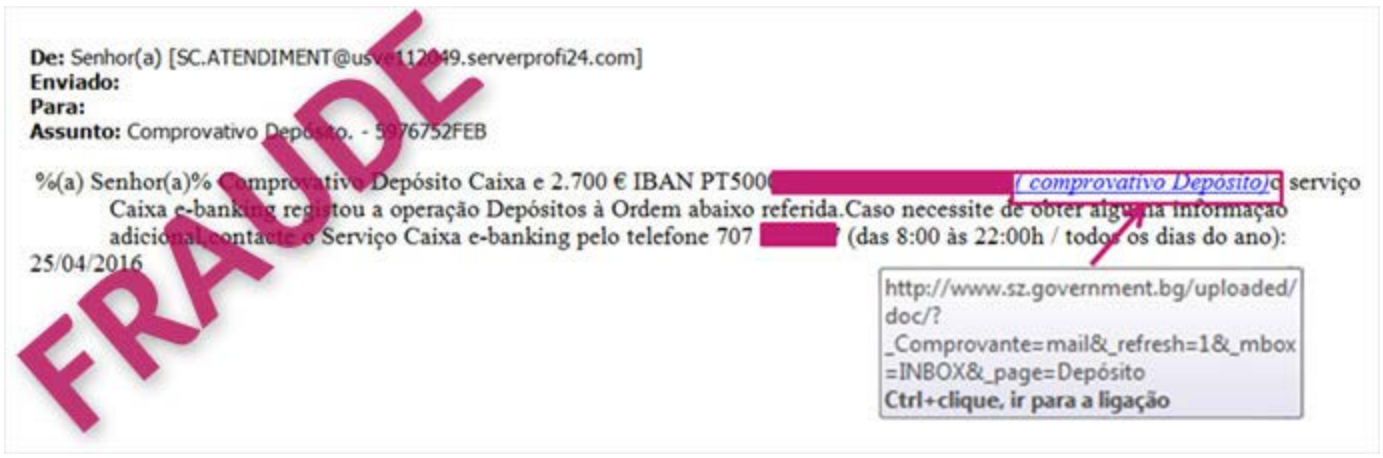
- Reduza o *spam* (mensagens de correio eletrónico não solicitadas e relacionadas com publicidade, são enviadas em quantidade massiva com o objetivo de divulgar serviços ou produtos e não só…);
- Mantenha o filtro de *spam* ligado;
- Suspeite de publicidade e ofertas não solicitadas bloqueando o endereço do remetente;
- Esteja atento ao conteúdo das mensagens de correio eletrónico caso não reconheça os remetentes;
- **Uma instituição bancária nunca lhe irá pedir a confirmação de dados sensíveis**, como códigos de acesso ou dados pessoais **(ex: número de telemóvel ou número do cartão de crédito)** através de uma mensagem de correio eletrónico;
- Elimine de imediato qualquer mensagem de correio eletrónico suspeita sem abrir quaisquer anexos ou aceder a *links*.

Uma mensagem de correio eletrónico não fidedigna pode parecer ter sido remetida por uma entidade confiável. Contudo, fique alerta para alguns sinais:

- O domínio do endereço remetente é gratuito e não um domínio oficial de uma entidade, organização ou empresa (por exemplo, **o domínio do Millennium bcp é @ millenniumbcp .pt**);
- Inicia com uma saudação genérica, não é personalizada, bem como, contém erros ortográficos ou gramaticais (por exemplo “Querido Cliente”);
- Carece de uma ação inadiável, por exemplo, que a sua conta não está segura, que pode ser encerrada ou que tem uma dívida para liquidar;
- Solicita informações pessoais, como o seu nome, códigos de acesso ou dados de cartões bancários;
- Inclui um *link* para um site com uma URL (endereço web) diferente do endereço oficial da entidade.

Exemplos de mensagens fraudulentas recentes:





Navegue com segurança:

- Verifique se a URL, na barra de endereços do navegador, contêm erros ortográficos ou nomes inesperados, conforme os exemplos que disponibilizamos acima;
- Desconfie caso o site que esteja a consultar não identifique contactos;
- Antes de fornecer dados pessoais ou financeiros **verifique se o endereço da página é confidencial e que está num ambiente seguro (https:// + cadeado)**;
- **Nunca aceda a sites bancários através de *links*, motores de pesquisa ou, mesmo, através da opção "Favoritos"**. Digite sempre o endereço completo na barra de endereços**.**

Mantenha o seu computador protegido contra software malicioso e outros problemas técnicos usando:

- Firewall;
- Software antivírus;
- Sistema operativo atualizado;
- Ferramentas anti-malware.

Outras medidas de segurança que pode adotar:

- Utilize sempre uma rede segura para aceder a sites bancários ou efetuar compras online;
- Bloqueie o navegador a pop-ups ou use navegadores diferentes;
- Abra só os anexos se foram enviados por pessoas/entidades que conhece e confia;
- Crie códigos de acesso fortes - evite usar datas de nascimento, números de telemóvel, números sequenciais

(ex:11111111), etc;
- **Os seus códigos de acesso são secretos, pessoais e intransmissíveis - não os partilhe!**

Para que possa acompanhar os incidentes de segurança que possam interferir na utilização do seu computador ou equipamento móvel e nos canais automáticos do Millennium bcp consulte as nossas Newsletters e a informação que disponibilizamos em Avisos de Segurança, ambos disponíveis para consulta no site do Millennium bcp, menu M » Tudo sobre: Segurança.

LEMBRE-SE QUE...

Se verificar alguma situação anómala em millenniumbcp.pt 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

siga-nos no facebook

Esta informação é da responsabilidade do Millennium bcp.

será de 0.25 €. A estes valores acresce o respetivo IVA.

Estes e-mails não permitem o acesso direto 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 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 eletrónico, aceda ao Homebanking no site do Millennium bcp e, no menu "Área M", selecione a opção "Criar / Alterar e-mail".

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.094.235.361,88 euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa coletiva 501 525 882.

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

Versão portuguesa

Warnings such as “you should not share your access codes”, “you should not open links or executable files on suspicious e-mails” and that “e-mails sent by banking institutions never have links” are a constant, and it does not surprise anyone that banks regularly stress these and other warnings, on their websites, regarding untrustworthy e-mails, advising users on how to prevent becoming the target of cyber-crimes.

After all... technology is ever evolving and criminals are always finding new ways to manipulate it.

As internet users we must be vigilant and regularly adopt new safety measures, keeping in mind how important it is to protect our personal data as well as the devices we use.

For that purpose, here are some recommendations on how to keep information safe when you use the e-mail or go online:

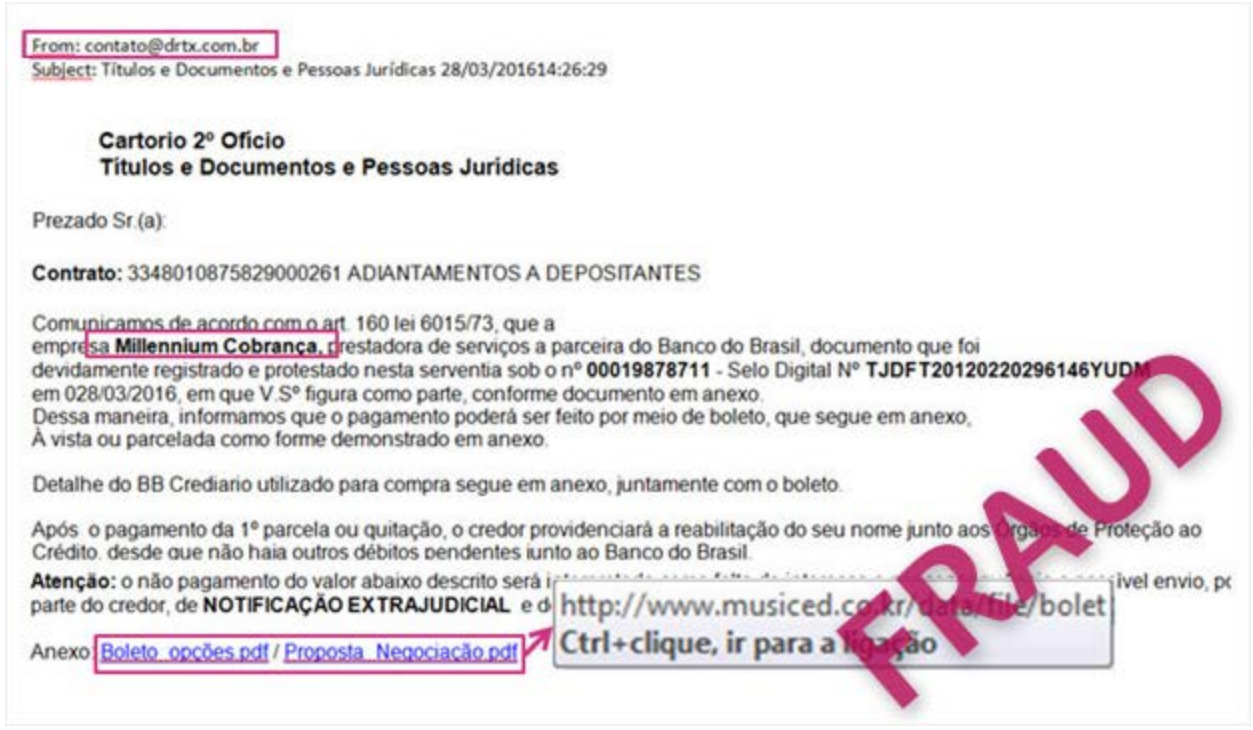
- Reduce spam (unrequested e-mails connected to advertising, sent massively to promote products and other things...);
- Keep your spam filters on;
- Be suspicious of unrequested advertisements and offers, and block the sender's address;
- Pay attention to the content of the e-mails if you do not recognize who sent them;
- **A bank will never ask you for the confirmation of sensitive data**, such as access codes or personal data **(ex. mobile phone nr. or credit card nr.)**, by e-mail;
- You should immediately delete any suspicious e-mail without opening attachments or links;

A fraudulent message may look as if it was sent by a trustworthy entity. Yet, you should always pay attention to some signs:

- The sender's e-mail provider is a free host and not the official domain of an entity, organization or company (for instance **Millennium bcp's domain is @ millenniumbcp .pt**);

- It opens with a generic greeting, is not personal (for example “Dear Customer”), and shows spelling errors and/or bad grammar;
- The message requires that you do something urgently, claiming for instance that your account is not safe, that it could be closed, or that you have a debt to pay;
- It requests personal information such as your name, access codes or data on your bank cards;
- It includes a link to a website with an URL (web address) that differs from the entity's official website.

Here are some examples of recent fraudulent messages:



Go online with safety:

- Check the URL in the browser address bar and look for any spelling mistakes or unexpected names as shown in the examples above;
- Be suspicious if the website you are visiting does not provide contact information;
- Before you provide personal or financial data check the address and **make sure you are on a confidential and secure webpage (https:// + lock)**;
- **You should never open bank websites through links on messages, search engines or even through your "Favorites"**. Always type the complete address on the address bar.

Keep your computer safe from malicious software and other technical problems by:

- Using a Firewall;
- Installing an antivirus;
- Updating the operating system;
- Using anti-malware tools.

Some other security measures you can use:

- Always use a secure network connection to open bank websites or making purchases online;
- Block pop-ups on your browser or use different browsers;
- Only open attachments sent by people/entities you know and trust;
- Create strong access codes - avoid using birth dates, mobile phone numbers, sequential numbers (ex: 11111111), etc.;
- **Your access codes are secret, personal and non-transmissible - please don't share them!**

To keep up with security incidents that may interfere with using Millennium bcp's website on your computer or mobile phone, or with the use of automatic channels, please read our Newsletters and the information we provide on our Security Warnings, all available at Millennium bcp's website, M tab » All about: Safety.

Source: Millennium bcp

REMEMBER...

If you ever find something out of place at www.millenniumbcp.pt or on Millennium bcp's 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 resposible 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.