

English version



Especial “Dia da Internet Segura”

No passado dia 7 de fevereiro de 2017 comemorou-se o Dia da Internet Segura (Safer Internet Day) sob o tema “Marca a Diferença: Unidos por uma Internet Melhor!”, coordenado pela InS@fe / INHOPE, com o apoio da Comissão Europeia e financiado pelo programa CEF - Connecting Europe Facility.

Esta iniciativa promove a consciencialização sobre os riscos e a responsabilidade na utilização da Internet e é dirigida especialmente a alunos, professores, assistentes, encarregados de educação e pais.

A Internet mudou drasticamente a maneira como interagimos com o mundo, nomeadamente, nas crianças e jovens. Através deste canal podem obter ajuda para os trabalhos escolares, expressar-se criativamente, contactar amigos ou familiares e esclarecer dúvidas.

Contudo, a Internet também oferece riscos, nomeadamente em temas como:

- *Cyberbullying*;
- Exposição a material inadequado;
- Predadores online;
- Disponibilização de informação pessoal.

Neste sentido, é necessário o envolvimento de todos os que participam na educação da criança ou jovem sensibilizando, criando hábitos e colocando em prática regras que visam a sua segurança.

Este ano, os temas centrais do Dia da Internet Segura foram as redes sociais, os jogos online, as relações online e a adição (também) online.

É preciso falar sobre os riscos da utilização da Internet e ensinar as crianças e jovens a enfrentar eventuais situações desagradáveis.

Por exemplo, nas redes sociais deve-se ensinar a ativar as definições de segurança para acessos e logins, definir os dispositivos reconhecidos e os contactos seguros, limitar o acesso de terceiros às publicações pessoais e rever todas as publicações em que for identificado, de entre outras opções e definições disponíveis.

Sobre os jogos online, e caso não exista a supervisão de um adulto, existe o risco de acederem a conteúdos inadequados, provocar reacções violentas e sintomas de adição, para além de existir a possibilidade de contacto com estranhos, bem como, a surpresa (desagradável) de ter custos associados. Confirme que o jogo é adequado à idade, controle o tempo que a criança passa online e se o jogo, não obstante ser gratuito, permite fazer compras (por exemplo, a extensão do jogo).

Não podemos esquecer que o acesso à Internet também pode causar dependência, a adição online, pelo que deve ficar atento a alguns sinais:

- Ansiedade;
- Sonha com jogos de forma regular;
- Isolamento, dedica mais tempo a utilizar a Internet do que na realização de outras tarefas;
- Falta de interesse pela escola;
- Vida social reduzida.

Já ouviu falar em termos como *sexting/frexting*, *grooming*, *sextortion*? Faça uma pesquisa sobre estes tipos de crimes que ocorrem na Internet e adote um diálogo contínuo sobre a segurança nas relações *online*, recordando que:

- Não deve fornecer informações pessoais, como a morada, número de telefone, passwords, ou outras informações pessoais, mesmo aos melhores amigos;
- Deve falar imediatamente com um adulto caso se depare com algo estranho ou que o coloque numa situação desconfortável;
- Não deve marcar encontros com amigos virtuais (desconhecidos);
- Não deve publicar fotos pessoais ou de outras pessoas sem o prévio consentimento de um adulto;
- Não deve responder a mensagens e/ou solicitações recebidas via email, online ou através das redes sociais, que o coloquem numa posição desconfortável. Caso o faça, deve falar imediatamente com um adulto;
- Não deve fazer downloads sem saber exatamente o que está a ser transferido. Esta ação pode comprometer o computador ou dispositivo móvel;
- Não deve publicar ou fazer comentários online, ou mesmo enviar mensagens, que possam ferir a suscetibilidade de outras pessoas (Cyberbullying).

Lembre-se que... o acompanhamento da criança ou jovem no acesso à Internet permite:

Educar, monitorizar e, como consequência, mantê-la em Segurança!


No acesso ao homebanking do Millennium bcp **NUNCA solicitamos o seu número de telemóvel ou a instalação de software/programas de segurança.**

É necessário ler atentamente o conteúdo dos SMS's com os Códigos de Autorização, antes de confirmar uma operação no homebanking.

Aproveitamos para alertar para o conteúdo de mensagens fraudulentas detetadas recentemente, as quais afetam o equipamento do utilizador e, por consequência, alteram as páginas de acesso ao site do millenniumbcp.pt

Exemplos das mensagens:

From: Autoridade Tributária e Aduaneira [mailto:Roberto@autoridadeaduaneira.loan]
Sent: Monday, January 30, 2017 8:26 AM
To:
Subject: Assunto Importante


AVISO IMPORTANTE


Exmo(a) Senhor(a)

Está em curso o procedimento de actualização da Lista de Devedores na Internet.

Verifica-se que em seu nome existem processos de execução fiscal para cobrança de dívidas fiscais, que preenchem os requisitos para a inclusão na Lista de Devedores.

Assim, venho por este meio recomendar que proceda, o quanto antes, à regularização da sua situação tributária, procedendo ao pagamento da dívida, desse modo, ponto termo, ao procedimento de inclusão do seu nome na Lista de Devedores na Internet.

Total de débitos a partir de 30 de Janeiro de 2017 € 2419,68


DOWNLOAD e-fatura

https://lon02.objectstorage.softlayer.net/v1/AUTH_69e723b7-371c-454d-bca5-8d65df690e37/efaturaweb/E-Fatura_1827732.zip
 Clique para seguir ligação

Esta mensagem de correio eletrónico e qualquer dos seus ficheiros anexos, caso existam, são confidenciais e destinados apenas (x), podendo conter informação confidencial, privilegiada, e que não deverá ser divulgada, copiada, gravada ou distribuída nos termos da mensagem, ou se ela lhe foi enviada por engano, agradecemos que não faça uso ou divulgação da mesma. A distribuição ou utilização desta mensagem por engano, por favor avise-nos de imediato, por correio eletrónico, para o endereço acima e apague a cópia.

From: Millennium bcp [mailto:bcppt@setpsfipmm02.bcpcorp.net]
Sent: Tuesday, January , 2017
To:
Subject: nova mensagem

Você tem uma nova mensagem esperando por você na Caixa de entrada do NetBanco.
 Você pode visualizá-lo fazendo logon no HomeBanking

[Clique aqui](#)

From **Millennium bcp** <millenniumbcp@bell.net>
Subject: Re: Fwd: nova mensagem importante

Olá,

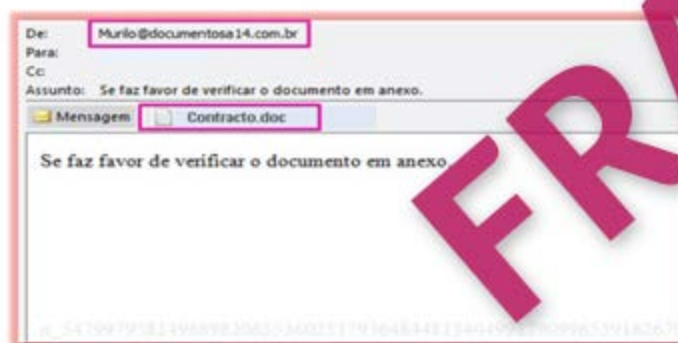
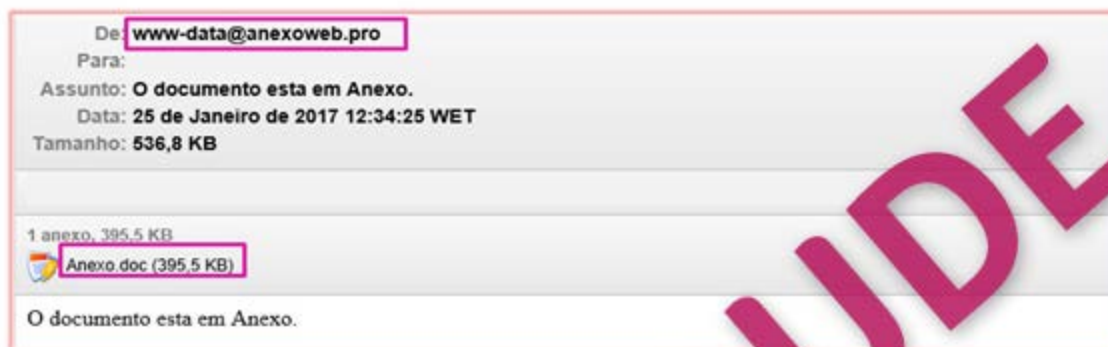
Seu conselheiro lhe enviou uma nova mensagem para ver a mensagem, por favor clique no link abaixo:

clique aqui

<https://www.elinord.se/pt/portugal>
Ctrl+clique para a ligação

cordialmente

Millenniumbcp.pt



Para informação adicional sobre estas mensagens de correio eletrónico fraudulentas, e outros temas de Segurança, aceda ao menu M » Tudo sobre: Segurança » Avisos de Segurança: Saber mais, em www.millenniumbcp.pt.

Recordamos que:

- Deve suspeitar de qualquer email que peça uma “ação imediata” e que contenha erros ortográficos/gramaticais ou anexos de ficheiros executáveis (.exe). Se necessário, confirme a sua origem junto da entidade que o envia;
- O acesso ao site do Millennium bcp é efetuado com o Código de Utilizador e três dígitos aleatórios do Código Multicanal (caso erre a introdução das posições, estas mantêm-se até que o login seja efetuado com sucesso);
- Deve ler atentamente o conteúdo dos SMS's recebidos com Códigos de Autorização, pois os dados da operação são identificados no texto da mensagem;
- O *phishing* visa confirmar/obter, de forma abusiva, dados pessoais/credenciais de acesso através de mensagens com

- links*/anexos que podem infetar o computador com software malicioso ou conduzir o utilizador a sites falsos, idênticos aos fidedignos. Evite seguir *links* para sites externos, bem como abrir ficheiros executáveis;
- Nunca faculte informação ou elementos de carácter pessoal como resposta a um e-mail;
 - Instale (caso ainda não o tenha feito) um *software* antivírus e efetue regularmente as atualizações do mesmo.

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



Esta informação é da responsabilidade do Millennium bcp.

Este e-mail é apenas informativo, por favor não responda para este endereço. Para obter esclarecimentos adicionais, sobre este ou qualquer outro assunto, ou efetuar 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).

Se ligar para 707 50 24 24 a partir da rede fixa terá um custo máximo de 0.10 € por minuto; se optar por nos ligar a partir da rede móvel o custo máximo por minuto 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](mailto: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 5.600.738.053,72 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.



Safer Internet Day Special

The Safer Internet Day was celebrated last 7 February 2017 with the theme of 'Be the change: Unite for a better internet!'. It is organised by the joint Insafe-INHOPE network, with the support of the European Commission, with funding provided by the Connecting Europe Facility programme (CEF).

This initiative aims to promote awareness of risks and responsibility while using the internet and especially targets students, teachers, carers, educators and parents.

The Internet has drastically changed the way we interact with the world, especially for children and young people. Through this channel they can get help with their homework, express themselves creatively, contact friends or family members and answer their own questions.

Yet, the internet also bears risks, especially the following:

- *Cyberbullying;*
- *Exposure to inappropriate material;*
- Online predators;
- Disclosing personal information.

Therefore, everyone takes part in the education of a child or young person by helping them become more aware, get better habits and by putting in place some rules for being safe.

This year the Safer Internet Day targeted social networks, online gaming, online relationships and (also) internet addiction.

One should talk to children and young people about the risks of going online and teach them to face unpleasant situations that may occur.

For example, when using social networks, teach them to activate security settings for access and login, define recognised devices and trusted contacts, limit public access to posts and review all posts where they are tagged, among other settings available.

Regarding online gaming, if there is no supervision from an adult, there is a chance children could gain access to inappropriate content, leading to violent reactions and addiction symptoms, besides the possibility of contact with strangers, as well as the (unpleasant) surprise of associated costs. Check if the game is age appropriate, control how much time the child is online and if

the game, despite being free, requires purchases (such as the game extensions).

We cannot forget that internet access can also cause addiction, therefore you should pay close attention to some signs:

- Anxiety;
- Dreams are regularly game related;
- Isolation, spends more time online than on other activities;
- Lack of interest in school;
- Decreased social life.

Have you heard the words *sexting/frexting*, *child grooming*, *sextortion*? Research these crimes that take place online and try to establish a continuous dialogue about how to establish safe online relationships, reminding them that they:

- Shouldn't give away personal information, such as their address, phone number, passwords or other personal information, even to their best friends;
- Should immediately speak with an adult if they find something strange or that puts them in an uncomfortable position;
- Must not arrange to meet virtual friends (strangers);
- Must not disclose personal photos or photos of other people without the approval of an adult;
- Shouldn't answer messages and/or requests received online, by e-mail, or through the social networks that put them in an uncomfortable position. If they do this, they should speak with an adult immediately;
- Shouldn't download anything without knowing exactly what is being transferred. This could compromise the computer or smartphone;
- Shouldn't post or make comments online or even send messages that may offend or hurt other people (Cyberbullying).

Remember that... monitoring internet use by children/teenagers enables you to:

Educate, monitor and, consequently, keep them Safe!

Source: Millennium bcp

REMEMBER...

M

To access Millennium bcp's homebanking services, the Bank **NEVER requests your mobile phone number or the installation of security software.**

You should carefully read the contents of the SMSs with Authorisation Codes, before confirming a transaction on the website.

We also wish to warn you about the contents of fake messages recently found that tamper with the user's device and therefore alter the pages that open the millenniumbcp.pt website.

Example of the e-mails received:

From: Autoridade Tributária e Aduaneira [mailto:Roberto@autoridadeaduaneira.loan]
Sent: Monday, January 30, 2017 8:26 AM
To:
Subject: Assunto Importante



AVISO IMPORTANTE

Exmo(a) Senhor(a)

Está em curso o procedimento de actualização da Lista de Devedores na Internet.

Verifica-se que em seu nome existem processos de execução fiscal para cobrança de dívidas fiscais, que preenchem os requisitos para a inclusão na Lista de Devedores.

Assim, venho por este meio recomendar que proceda, o quanto antes, à regularização da sua situação tributária, procedendo ao pagamento da dívida, desse modo, ponto termo, ao procedimento de inclusão do seu nome na Lista de Devedores na Internet.

Total de débitos a partir de 30 de Janeiro de 2017 € 2419,89

DOWNLOAD



https://lon02.objectstorage.softlayer.net/v1/AUTH_69e723b7-371c-454d-bca5-8d65df690e37/efaturaweb/E-Fatura_1827732.zip
Clique para seguir ligação

Esta mensagem de correio eletrónico e qualquer dos seus ficheiros anexos, caso existam, são confidenciais e destinam-se apenas a (s), podendo conter informação confidencial, privilegiada, a qual não deverá ser divulgada, copiada, gravada ou distribuída nos termos da mensagem, ou se ela lhe foi enviada por engano, agradecemos que não faça uso ou divulgação da mesma. A distribuição ou utilização não autorizada desta mensagem ou dos seus anexos constitui uma violação da política de segurança da informação da empresa. Se recebeu esta mensagem por engano, por favor avise-nos de imediato, por correio eletrónico, para o endereço acima e apague a cópia da mensagem e dos seus anexos.

From: Millennium bcp [mailto:bcppt@setpsfipmm02.bcpcorp.net]
Sent: Tuesday, January , 2017
To:
Subject: nova mensagem

Você tem uma nova mensagem esperando por você na Caixa de entrada do NetBanco.
Você pode visualizá-lo fazendo logon no HomeBanking

[Clique aqui](#)

From **Millennium bcp** <millenniumbcp@bell.net>
Subject: Re: Fwd: nova mensagem importante

Olá,

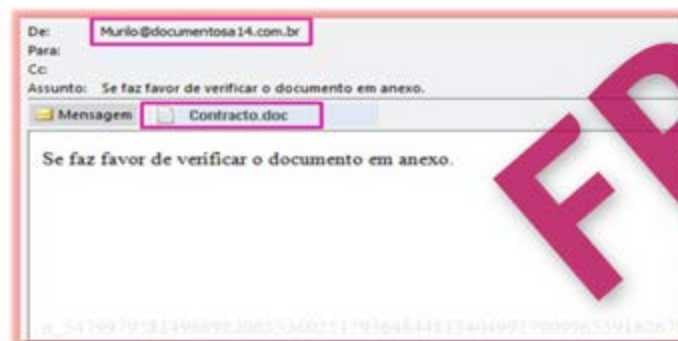
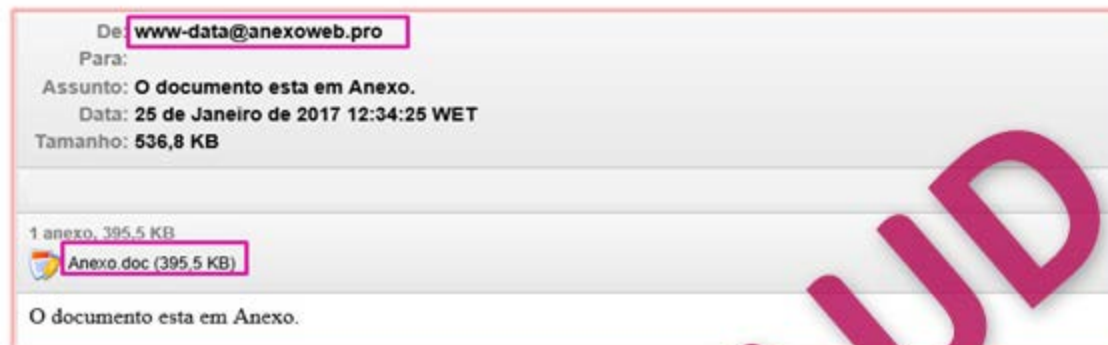
Seu conselheiro lhe enviou uma nova mensagem para ver a mensagem, por favor clique no link abaixo:

[clique aqui](#)

<https://www.elinord.se/.../portugal>
Ctrl+clique, ir para a ligação

cordialmente

Millenniumbcp.pt



You can get more information on these fake e-mails and other security issues in the security area, clicking on the M tab - All about: Security» Security Notices: Learn more.

Please be reminded that:

- You should beware of any e-mail that requires "immediate action" and shows spelling errors or bad grammar or has attached executable files (.exe). If necessary, confirm the source with the sender;
- Millennium bcp's website is accessed using a User Code and three random positions of the Multichannel Code (if you enter a wrong number, the three random positions requested remain the same until you login successfully);
- Carefully read the SMS received containing the Authorisation Codes since the transaction data are identified in the text message;
- Phishing aims to abusively confirm/get personal data/access codes through messages with links/attachments that can infect a computer with malicious software or lead the user to fake websites, identical to the trustworthy websites. Avoid opening

- links to external websites as well as opening executable files;
- Never provide personal information or data in an e-mail reply;
- Install (if you haven't done so yet) an antivirus software and update it regularly.

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 @ millienniumbcp.pt](mailto: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".

Banco Comercial Português, S.A. Company open to public investment Registered Office: Praça D. João I, 28 - Porto. Share Capital: 5.600.738.053,72 euros Registered at the Companies Registry Office of Oporto. Single registration and tax identification number 501 525 882.

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