

Caso não consiga visualizar correctamente este e-mail por favor reporte-nos esta situação para: informacoes.clientes@millenniumbcp.pt

In case you don't see this e-mail correctly, please report the situation to: informacoes.clientes@millenniumbcp.pt

Millennium
bcp

Newsletter sobre Segurança

Microsoft®

Dezembro 2007 - nº 43

[English version](#)

%%Exm%%
%%customerName%%

A primeira edição desta **Newsletter de Segurança** remota a Junho de 2004. Desde então, muitos têm sido os temas e os assuntos abordados com o intuito de contribuir para reforçar os mecanismos de segurança, na utilização dos sistemas informáticos, com especial incidência sobre a Internet.

- Verifique se está o mais seguro possível
- Spam e vírus aumentam na época de Natal

A partir de 2008 daremos continuidade a este pressuposto - inerente à criação desta Newsletter - mas chegaremos até si com a **periodicidade trimestral**.

A findar 2007 e nesta última edição mensal, "**Em Destaque**" deixamos-lhe uma *checklist* de procedimentos que deverá verificar se os cumpre.

Em "**Princípios Básicos de Segurança**" e, ainda, sob o mote da quadra Natalícia saiba que as mensagens de correio não solicitadas (*Spam*) aumentam, em média, cerca de 200% face ao resto do ano e, conseqüentemente, a exposição a vírus ou outro tipo *software* malicioso. Recorde alguns cuidados a ter.

Boa leitura e excelente 2008.



Em Destaque

Verifique se está o mais seguro possível

Depois de muitas Newsletters de aconselhamento sobre boas práticas de segurança, chegou o momento de verificar se cumpre, ou não, esta *checklist* com os principais cuidados a ter, para sua segurança:

Códigos de acesso ou *passwords*

- Códigos de acesso distintos para os diferentes serviços (banca *online*, correio electrónico, entre outros...);
- Não são utilizados nomes, datas relevantes ou dados pessoais;
- Os códigos de acesso têm mais de 7 caracteres, utilizando maiúsculas e minúsculas, números e/ou outros símbolos;
- Os códigos de acesso são alterados periodicamente;
- Os códigos de acesso não se encontram guardados no computador ou noutros locais de acesso fácil.

Segurança do computador

- O sistema operativo e demais programas encontram-se actualizados;
- O antivírus está instalado e actualizado;
- A *firewall* está instalada e a funcionar correctamente;
- Na utilização de serviços garantir a segurança da ligação(<https://>);
- Os principais ficheiros e documentos têm cópia de segurança.

Correio Electrónico

- O remetente da mensagem é conhecido e a informação não é duvidosa;
- Verificar a existência de vírus ou aplicações prejudiciais ao computador antes de abrir ou executar os ficheiros;
- Os *links* constantes da mensagem devem ser digitados no navegador de Internet.



Spam e vírus aumentam na época de Natal

Ainda se recorda da última vez que colou um selo para enviar um postal de Boas Festas?

O Natal e o fim do ano são épocas tipicamente movimentadas em todas as caixas de correio electrónico, sendo por isso aconselhável prevenir os utilizadores de Internet para a sua maior exposição ao *Spam* (mensagens de correio electrónico não solicitado) e a vírus.

Durante o período das festividades que se aproximam, as mensagens de correio não solicitadas aumentam, em média, cerca de 200% face ao resto do ano.

De acordo com os dados da Symantec, desde 2006 que o *spam* não pára de aumentar... já nesse ano, em média, a quantidade de mensagens *spam* havia superado a quantidade de mensagens normais registando valores de 56% do e-mail total. No entanto é em 2007 que o aumento se substancia com valores de 72%, quase $\frac{3}{4}$ de todo o e-mail mundial.

Será necessário estar particularmente atento a técnicas como o *phishing*, o *spyware* e o *adware*. O número de mensagens de correio electrónico não solicitado, dissimulando ataques de *phishing*, também aumentaram exponencialmente durante os últimos anos. Como já foi referido em edições anteriores desta Newsletter, o *phishing* visa roubar dados pessoais através de mensagens que conduzem o utilizador a sites falsos, cópias fiéis daqueles a que acede habitualmente, solicitando a introdução de dados confidenciais.

O *spyware* e *adware* são igualmente manobras típicas de disfarce da origem das mensagens que permitem aos seus autores reunir dados sobre os gostos dos utilizadores, tipicamente usadas para fins publicitários ou ilegais.

Assim, e como o perigo continua à espreita nas caixas de correio electrónico de cada um, voltamos mais uma vez a alertar para o facto de muitas das mensagens (supostamente inocentes) que circulam nesta altura do ano poderem conter vírus (ou outro qualquer *software* malicioso), aproveitando a circunstância de os utilizadores se encontrarem mais susceptíveis a abrir, sem prevenção, qualquer mensagem recebida. Nunca será demasiado relembrar a necessidade de se manter vigilante para esta "vaga de virose natalícia".

Tal como em relação às gripes, comuns nesta altura do ano, convém também tomar algumas medidas de bom senso para combater os vírus informáticos natalícios que chegam pela Internet.

- Analise as mensagens de Correio electrónico que recebe antes de abrir;
- Nunca faculte dados confidenciais;
- Ao aceder a páginas de acesso confidencial, confirme o endereço e certifique-se que está num ambiente seguro (o endereço que lhe é apresentado no *browser* começa por <https://> e no canto inferior direito surge um cadeado);
- Instale um *software* antivírus e efectue regularmente actualizações do mesmo.



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 ou ligue para o número de telefone 707 50 24 24.

Estes e-mails não permitem o acesso directo ao site 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

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço electrónico, aceda a www.millenniumbcp.pt e escolha a opção Contas e, posteriormente, a opção Personalização.

Millennium
bcp

Security Newsletter

Microsoft®

December 2007 - n° 43

[Versão Portuguesa](#)

%%Exm%%
%%customerName%%

The first issue of our **Security Newsletter** dates back to June 2004. Since then, we have written about all kinds of issues so that you could learn how to use IT systems - namely the internet - more safely.

As of 2008 we will continue to follow up on this project - which was at the very root of the creation of this Newsletter - but on a quarterly basis.

Closing 2007 and this last monthly issue, we leave you, in "**Highlights**", a very useful checklist.

In "**Basic Security Principles**", learn that during the Christmas season spam increases on average about 200% compared to the rest of the year. As a result, so does exposure to viruses and malware. Keep our tips in mind.

Enjoy your reading and Happy New Year.



Highlights

- [Make sure you are safe](#)
- [Spam and viruses increase during Christmas season](#)

Make sure you are safe

After several Newsletters on safety procedures, we now leave you with a checklist for you to confirm if you are indeed following security guidelines:

Access Codes or Passwords

- Use different access codes for different services (online banking, email, etc...);
- Do not use any names, special dates or personal details · Access codes must contain more than 7 characters, including caps and lower case, numbers and/or other symbols;
- Change your access codes on a regular basis;
- Do not store access codes on your PC or other easily accessible places.

Computer Security

- Keep your operating system and software updated;
- Check antivirus is installed and updated;
- Check firewall is installed and operating correctly;
- Use only services with secure connections (https://);
- Backup your main files and documents.

Emails

- Make sure you know who the sender is and the message contents are trustworthy;
- Scan for viruses and malware before opening or running files;
- Do not click on links - type them into your browser.



Basic Security Principles

Spam and viruses increase during Christmas season

Do you remember the last time you put a stamp on an Xmas Greetings postcard?

Christmas and New Year's is an extremely busy emailing season. Web surfers should be on alert regarding the greater risk of exposure to spam and viruses.

During these upcoming Holidays, spam basically doubles compared to the rest of the year.

According to Symantec, spam messages have been steadily increasing since 2006... even back then, the amount of spam had already risen above the volume of regular emails: totalling 56% of all emails. In 2007 this increase has reached 72%, just under ¾ of all emails across the globe.

Special attention is due to techniques such as phishing, spyware and adware. The amount of spam covering for phishing attacks has also increased exponentially in the last years. As mentioned in previous issues of this Newsletter, phishing aims to steal personal details through messages which lead the user into fake sites. These are usually good imitations of sites you regularly access, wherein you are asked to enter confidential information.

Spyware and adware are also typical manoeuvres to mask the origin of messages which allow their authors to collect data on users' habits, then typically used for advertising or illegal purposes.

On this account, and since danger lurks in all our inboxes, we'd like once more to alert you to the number of (supposedly innocent) messages circulating at this time of year that might contain a virus (or malware). These emails take advantage of the fact that users are more likely, during this season, to unwarily open emails.

We cannot underline enough the need to stay on the lookout for this 'Xmas virus wave'.

As with the flu, so common at this time of year, it is also prudent to take some measures against the Christmas viruses that come to visit us over the internet.

- Scan your email before opening it;
- Never give out confidential information;
- When accessing restricted pages, check the address and make sure you are operating in a secure environment (the address in your browser should start with https:// and a padlock should appear on the bottom right-hand corner);
- Install antivirus software and update it regularly.



www.millenniumbcp.pt

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

***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 or dial 707 50 24 24.*

These emails do not grant direct access to 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

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 and click on Accounts, then Customize.