



December 2006 - n° 31

We are pleased to provide two articles in this newsletter that we believe are of great importance during this Christmas season.

- [Fraud in online donations](#)
- [Christmas Season: Preparing a new computer for the Internet](#)

**Highlights** provides advice to avoid fraudulent schemes linked to online donations. During this season many people use the Internet to make donations to help organisations of a humanitarian nature of various types. If you do, take care not to become a victim of fraudulent online requests for aid.

In **Basic Security Principles** find out what to do to prepare a new computer for the Internet if you were fortunate enough to receive one as Christmas gift.

A Happy Christmas!  
We'll be back with you in January!



## Highlights

### Fraud in online donations

Most fraudulent online donation schemes come in the form of e-mail spam messages and online forums, in which requests are made for donations in the name of the victims, to provide aid and funds for survivors or specifically for legitimate, well-known charity institutions.

A new form of fraud known as phishing is a type of spam or pop-up window that purports to be from a legitimate organisation but is used to try to get money or personal information from unwary users. Electronic phishing messages are becoming increasingly sophisticated and establish links to fake sites or sites whose origin is hidden, though they seem to be official. Phishing can also take place over the phone, so beware of charity-related requests over the phone.

### Advice to help you to avoid fraudulent online schemes

- Improve the security of your computer and use up-to-date technology to help block spam;
- Be careful if you receive an e-mail from a humanitarian organisation asking for cash. Don't jump in and click on any link or provide any personal information;
- Instead of replying to these requests, contact well-known, established humanitarian organisations to which you or people on whom you can rely have contributed;

- If you receive a request via e-mail from a charity institution that you would like to help, visit its Web site or ring them up to check the veracity of the request and find out how to contribute;
- When online type in the whole of the address of the humanitarian aid organisation in your Internet browser;
- Check whether the name of the organisation's Web site is correct and always check the Internet address before continuing to navigate around a Web site. Web sites containing hidden contents often use deliberate typing errors, easily missed, to mislead users;
- Be wary of e-mail messages from unknown origins, especially if they have photographs attached that could well be infected with computer viruses;
- If you provide your credit card number or personal information to a Web site related with charities, check that it makes use of updated encryption technology and that the site states its policy concerning the protection of personal information;
- Keep yourself up to date in respect of the most recent online fraud schemes through reliable providers of news on technology, governmental agencies and other professional sources.

Continue to donate, but take care!



## Basic Security Principles

### Christmas Season: Preparing a new computer for the Internet

When setting up a computer for the first time, check that the system comes complete with security software and that it has the most recent updates to help protect you against viruses and other potential threats, before you hook up to the Internet.

After connecting for the first time, it is also important that you update your operating system and the antivirus software regularly.

The following steps can help you to install the most recent security tools on your new computer, protecting it before accessing the Internet:

- **Make an inventory:** Consult the inventory or list of components supplied with the computer, to check that the hard disk contains all the software on the list and that the original installation CDs are available;
- **Record all the system information:** it's a good idea to keep a record of the computer's system information, should a computer technician need it later. To do so:
  - Click on **Start**;
  - Click on **Run** and write "msinfo32" in the text field;
  - Click on **OK** to open the System Information window;
  - Click on **File** on the menu bar and select Export from the menu;
  - Assign a name to the file and keep it stored on an external support such as a blank CD or diskette. Keep it in a safe place.
- Check the firewall;
- Adjust the privacy definitions: on the Internet Explorer **Tools** menu click on **Internet**

**Options** to open the Internet Options window. Using the **Privacy** tab you can adjust the way in which your computer deals with **cookies**;

- Download software updates: Activate Automatic Windows Updates and the automatic updating of your antivirus software (consult the manual that comes with it); Connect the modem or the network cable to access the Internet and run the Network Connection Assistant; When you are connected wait for Windows Update to install the latest software and security updates.

Having followed this advice enjoy your computer be it for entertainment or for professional purposes!



[www.millenniumbcp.pt](http://www.millenniumbcp.pt)

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



"Best Corporate/Institucional Internet Bank" Empresas em Portugal - "Best Consumer Internet Bank" Particulares em Portugal - "Best Bill Payment and Presentment" na Europa - "Best Information Security Initiatives" na Europa - "Best Online Deposits Acquisition" na Europa