

%%**Exm**%%
%%**customerName**%%

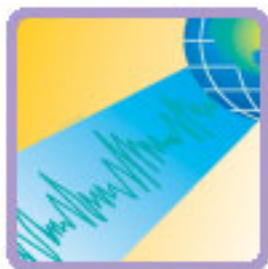
This month we discuss the security in the use of mobile phones and PDA's. Their inherent functionalities grow exponentially, especially the capabilities which exist for interconnection with a personal computer or with a computer network.

In this context, and so that you are confident in their respective use, this Newsletter contains information and practical guidance which we trust you will once again find useful.

Highlights:

Avoid being raided via your Bluetooth mobile phone

The Bluetooth® wire less technology is supplied with many mobile phones and PDA's. It was initially conceived to exchange documents between Bluetooth devices without



the use of encumbering connection cables, but has been expanded to supply other services, such as Web connections and online games. However, every time you transmit information online you may be vulnerable to online raids. And, with the increase in the popularity of Bluetooth, there is a proportionate increase in the interest of cyber-criminals.

When it is in the "visible" mode, your Bluetooth mobile phone or PDA sends... >>

News:

Check the security certificate before inserting financial or personal data in a Web site!

Recent technological innovations have facilitated the possibility of enjoying the advantages of making telephone calls over the Protocol... >>



Basic Security Principles:

Know how Mobile Banking works and what precautions should be taken

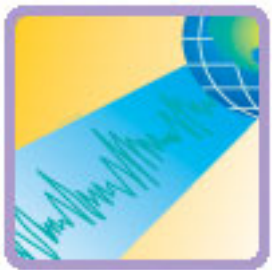
In our previous Newsletter we set you the challenge of testing your knowledge about security when using the Internet.... >>



Configuring and updating software:

Get a free security analysis for your computer

Windows Live Safety Center is a new tool which allows an analysis to your computer, helping its protection, cleaning and improved performance. This service is free and is directly available on the Internet by accessing ... >>



News:

Avoid being raided via your Bluetooth mobile phone

The Bluetooth® wire less technology is supplied with many mobile phones and PDA's. It was initially conceived to exchange documents between

Bluetooth devices without the use of encumbering connection cables, but has been expanded to supply other services, such as Web connections and online games. However, every time you transmit information online you may be vulnerable to online raids. And, with the increase in the popularity of Bluetooth, there is a proportionate increase in the interest of cyber-criminals.

When it is in the “visible” mode, your Bluetooth mobile phone or PDA sends a signal advising it is ready to be connected to another Bluetooth device and to transmit and receive data. However, any intruder which detects that signal may also try to join up with your unit and illicitly access your data in order to obtain your personal identification number (PIN).

The intruder, with your PIN, may:

- Steal information kept in your device, including contact lists, e-mails and text messages;
- Send unsolicited text messages or images to other Bluetooth devices;
- Obtain access to the controls of your mobile phone, thus enabling the intruder to make calls or send text messages from it, read and write contacts in your phone book, eavesdrop and connect to the Internet;
- Install a virus in your unit which could occasion the same damage as a computer virus – i.e., slow down or deactivate your service, or destroy and steal information.

Suggestions to improve your Bluetooth security:

- Maintain the Bluetooth definition in “not visible” (deactivated transmission) and only activate the “visible” mode when in use;
- Avoid keeping sensitive data, such as credit card numbers and passwords in any wire less device;
- Keep in touch with the developments and security problems of the Bluetooth technology and regularly contact the manufacturer of your device to find out the software updates or any specific security hazards.

And because we are discussing Security, be conversant with some of the terminology. Do you know the meaning of someone being Bluejacked?

Bluejacking is one of the many terms for Bluetooth raids:

- Bluejacking: send unsolicited text messages;
- Bluesnarfing: steal information;
- Bluebugging: steal mobile phone controls;
- War-nibbling: looking for Bluetooth signals to raid;
- Bluesniping: using a laptop and a powerful aerial to raid from a distance.





News:

Check the security certificate before inserting financial or personal data in a Web site!

Before inserting financial or personal data in a Web site, make certain that the site is secure. Using Internet Explorer you can do so through the icon

with a yellow padlock in the status bar on the lower side of your browser window.

A closed padlock indicates that the Web site uses encryption to help protect any personal confidential data which is introduced, such as credit card or identification numbers, or payment details.

Note that this symbol may not appear in all the pages of a site, but normally only in those pages which request personal information.

It is very unfortunate, but even the padlock symbol can be falsified.

To increase your security, double click the icon to view the site's security certificate. The name which follows "**Issued for**" must be the name of the site. Should it differ, you may have accessed a false site, also known as "spoofed", or with hidden contents.

If you are not certain as to the site's legitimacy, do not insert any personal information.

Play it safe and leave the site!

Advice: If you cannot visualize the status bar in the lower side of your browser window, click View in the upper side and select Status Bar to activate it.

top



Basic Security Principles:

Know how Mobile Banking works and what precautions should be taken

In our previous Newsletter we set you the challenge of testing your knowledge about security when using the Internet.

The Customer has currently at his disposal several means to contact his Bank, without the need to visit the Branch. After electronic tellers, better known as Automatic Cash Machines, and access to Internet Banking, **Mobile Banking** is now available in our every day life.

This is a service which allows you to access your accounts and to perform the main banking operations, in any place and at any time. All you need is a mobile phone or a PDA.

We suggest that, after accessing the Millennium bcp site, you visit the Mobile Banking area so that you find out how it works, how you can activate the service and which banking operations are available.

It is however always important that you take some security precautions and some preventive measures, and we thus recommend:

- Avoid that your mobile phone or PDA – which is in active service – be accessible to third parties who, although unable to effect banking operations in your name, will be able to access your accounts for information. To safeguard this possibility you may opt for an access PIN to the application (in this case you will not be able to access any information kept in the

Smartphone/PDA);

- Delete the messages with confidential information in your mobile phone, since these may be viewed by third parties which have access to it;
- Should you lend your PDA or Smartphone to another user of the Millennium bcp site, delete local data – through the “Personalization” option – since this can be viewed, even if accessed by a different user (this is safeguarded if the above referred PIN is used);
- Change your password and confirmation key from time to time, accessing the “Personal data” option in the www.millenniumbcp.pt site;
- In case the mobile phone is stolen when activated, ring telephone number 707502424, or deactivate the service in www.millenniumbcp.pt.

top



Configuring and updating software:

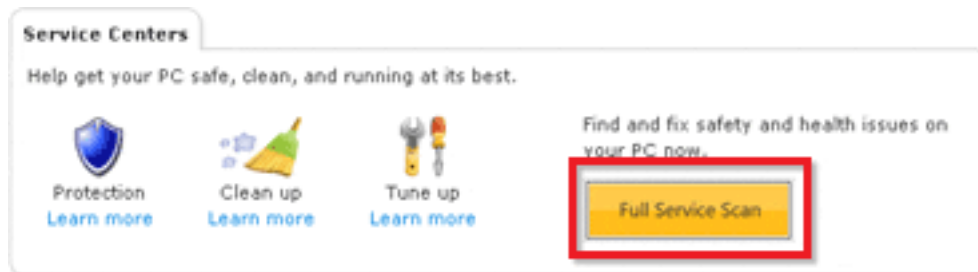
Get a free security analysis for your computer

Windows Live Safety Center is a new tool which allows an analysis to your computer, helping its protection, cleaning and improved performance.

This service is free and is directly available on the Internet by accessing <http://safety.live.com>. You can return to Windows Live Safety Center for further refinements, whenever you wish.

How to use Windows Live Safety Center

Visit **Windows Live Safety Center**, click on **Full Service Scan**, and follow the instructions on the screen.



The analysis programme of Windows Live Safety Center is downloaded and installed in your computer the first time you go through the analysis. This inspects your computer to detect virus, open ports, clean your disk and instal missing updates. When the analysis is completed it provides the results and any necessary advice.

top



"Best Consumer Internet Bank" em Portugal ● "Best Online Consumer Credit" na Europa
"Best Corporate/Institutional Internet Bank" em Portugal ● "Best Information Security Initiatives" - Particulares, na Europa
"Best Bill Payment and Presentment" na Europa ● "Best Information Security Initiatives" - Empresas, na Europa