

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

These days computers occupy an unquestionable place in our lives. We use them to perform countless tasks such as: financial transactions, which may be banking or just the purchase of products and services; communication, for example, through e-mails; data storage for personal or business use, etc. Their use, for whatever reason, should always be with the due precautions so as to avoid set-backs. We know that this is possible with just a little knowledge and so we have included some information we consider relevant for you here.

Highlights:

Videos on Security - Protect your privacy and your personal information online

Following on from previous editions, we wanted to highlight a new section on Microsoft's site dedicated to the topic of Security and which includes a series of short videos



which aim to help users to find out the most important security problems and how to avoid them.

This month our feature is on protecting privacy and your personal information online. The Internet facilitates operations such as shopping, performing banking operations and communicating online, but it also carries the risk of theft of identity. By taking some basic precautions, you can reduce your chances of becoming a victim.

Watch this video to learn more about this topic:
http://www.microsoft.com/athome/security/privacy/video_priv.msp

News:

VoIP: Your online telephone - Enjoy the advantages, know the risks

Recent technological innovations have facilitated the possibility of enjoying the advantages of making telephone calls over the Internet, also known as "Voice over IP" (or VoIP - Voice over Internet Protocol)... >>



Basic Security Principles:

Security Quiz

In our previous Newsletter we set you the challenge of testing your knowledge about security when using the Internet. Now spend some minutes of your time checking the correct answers... >>



Configuring and updating software:



Block Pop-ups with Internet Explorer

When you install SP2, the Pop-up Blocker is activated in Internet Explorer and is pre-configured to an average setting, which means that it will block most automatic Pop-ups... >>

News:



VoIP: Your online telephone - Enjoy the advantages, know the risks

Recent technological innovations have facilitated the possibility of enjoying the advantages of making telephone calls over the Internet, also known as

"Voice over IP" (or VoIP - Voice over Internet Protocol). You don't even have to have a computer to connect a "Voice over IP" network. However, as the service becomes more and more common, it has attracted the attention of online criminals and tricksters. Before trying a VoIP service, you should find out about the advantages and disadvantages of this system, and get to know the steps you should take to help to improve your security when you use the system.

Risks of Voice over IP systems:

- Theft: Intruders who may gain get into a VoIP server can gain access to filed voice data and to the service itself, using it to illegally listen into conversations or to use their account to make free calls
- Attack by a virus
- Non-regulated technology: for example, criminals may also use a process which goes by the name of caller ID spoofing (where the identity of the person making a call is hidden or camouflaged) in order to commit fraud.
They can do this by saying they are an official entity and attempt to find out sensitive information related with accounts.

Forms of protection when using the Voice over IP system:

- Use a router: An adapter is often supplied by the Voice over IP service provider, which brings the VoIP system directly to your fixed line telephone, without the need for a computer. This device helps to isolate your telephone against attacks and helps to protect your computer against viruses with which you may come into contact over the Internet;
- Keep your passwords safe: Create safe passwords to access Web sites of services which store your voice mail and other audio data. Do not disclose them to anyone;
- Keep your own computer secure.



Basic Security Principles:



Security Quiz

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

Now spend some minutes of your time checking the correct answers.

1. How does your computer get infected by a Virus?

- Executing an unknown program on a diskette or even on a CD-ROM;
- Installing programs from dubious sources opening files in Word, Excel, etc.;
- Opening documents in Word, Excel, etc. or documents attached to e-mail messages;
- All of the above**

A virus is a malicious code which attaches itself to a program or file, with the objective of being transmitted and propagating itself to third parties. It propagates the infection as it is transmitted from computer to computer. Viruses can damage your software, computer equipment and files. If you have not installed antivirus software, you may obtain this from a variety of companies. To find out more about special offers on antivirus and firewall packages, we would suggest you visit the Software and Security page on Microsoft's site: Transfers and tests

2. Which files can do the most damage?

- Those which end in .jpg, .gif, .mp3;
- Those which end in .exe, .com, bat and .vbs.**

3. Keyloggers - What are they?

- Antivirus software;
- Spyware type programs;**
- Programs for entertainment.

Spyware is software which gathers personal information without your knowledge or permission. You can be the target of spyware if you use file sharing programs, if you transfer free games from sites which you do not trust, or transfer other software from unknown sources. Here are a few resources to help you protect your computer from spyware.

Install anti-spyware software from

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

4. What is a Firewall?

- A cover for your computer to protect it from fire;
- A personal code allowing access to the Internet;
- Software or equipment which helps to protect a computer against malicious attacks.**

Connecting a computer to the Internet without a firewall is like leaving your keys in your car with the engine running and the doors unlocked while you go into a store. While you can enter and leave the store before anyone notices, you run the risk that someone will grab the opportunity. On the Internet, computer pirates, using viruses, worms and other malicious software take advantage of the fact that some users do not use a firewall by finding and taking control over unprotected computers. A firewall can help to protect your computer against these and other security attacks.

5. After I install antivirus software is my computer totally protected?

- a. True;
- b. **False.**

6. You can be infected with Spyware if:

- a. You transfer programs from unknown sources;
- b. You transfer music, films, games and other file sharing software on the Internet;
- c. You navigate on the Internet and visit sites of dubious origin;
- d. **All of the above.**

7. What should I do after I install antivirus software?

- a. **Install antivirus updates on a regular basis;**
- b. Nothing. I'm already safe;
- c. Install antivirus updates once a year;
- d. Install antivirus updates only when the computer is infected with a virus.

8. What should I do after reinstalling the operating system?

- a. Install all of the security updates provided by the supplier;
- b. Install an antivirus and the respective periodic updates;
- c. Install an anti-spyware program and the respective periodic updates;
- d. **All of the above.**

And to conclude, to properly protect your computer you should have:

- An active Firewall always connected to the Internet
- An up-to-date anti-virus program
- "Automatic Updates" should be active
- Automatic Updates can automatically transfer and install important security updates according to your definitions.
- An up-to-date anti-spyware program.



Block Pop-ups with Internet Explorer

When you install SP2, the Pop-up Blocker is activated in Internet Explorer and is pre-configured to an average setting, which means that it will block most automatic Pop-ups. The pre-definitions of the Pop-up Blocker allow you to see Pop-ups which open when you click on a hyperlink or on a Website button. The Pop-up Blocker also makes a sound and shows the Information Bar when a Pop-up is blocked. You can adjust these definitions so that the Pop-up Blocker functions as you wish.

To change the definitions for the Pop-up Blocker:

1. Open Internet Explorer;
2. In the **Tools** menu go to **Pop-up Blocker** and click on **Pop-up Blocker Settings**.

If you wish to see the Pop-ups on a specific Web site, write the address (or URL) of the site in the Web site address box to be allowed and click on **Add**.

Suggestion: To allow a site to show Pop-ups temporarily, click on the Information Bar when it informs you that a Pop-up has been blocked. Then click on **Temporarily allow Pop-up**.

To block Pop-ups even if these show up when you click on a hyperlink or on a Web site button:

1. Open Internet Explorer;
2. In the **Tools** menu go to **Pop-up Blocker** and click on **Pop-up Blocker Settings**;
3. Select the **High** setting in the box near the bottom of the dialogue box.

Note: If you want to see blocked Pop-ups when this setting is activated, keep the CTRL key pressed down while the window is open.

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