

The Internet (and its use) are increasingly familiar to children from an early age. Adults are thus charged with the important role - a role of the utmost importance let it be said, like so many others they perform - of helping younger children to acquire best-conduct habits and practices when "surfing on the Internet".

Take advantage of our advice and enjoy leisure hours with the kids.

## Highlights:

### Teach children how to improve their security on the Web

The Internet can be an excellent place for children to learn, to be entertained, to chat with school pals or simply to relax and explore. But, just as in the



real world, the World Wide Web can be a dangerous place for children. Before allowing your children to use the Internet without supervision draw up a set of rules to be agreed by everyone.

If you're not quite sure where to begin check out the following ideas on what to discuss with your children to teach them how to use the Internet safely... >>

## News:

### Telephone Phishing

Phishing schemes usually use e-mail to direct potential victims to fake Web pages. A new form of phishing has now appeared... >>



## Basic Security Principles:

### Browser hijacking

Highjacking is a common form of online attack in which the highjackers take control of your computer's Internet browser and alter its appearance.... >>



## Configuring and updating software:

### Improve your safety on the Internet and that of your mailbox

Evil-minded highjackers and virus creators can infect your computer, taking advantage of low-security definitions of your e-mail programme and Web browsing software ... >>



## Highlights:



### **Teach children how to improve their security on the Web**

The Internet can be an excellent place for children to learn, to be entertained, to chat with school pals or simply to relax and explore. But, just as in the real world, the World Wide Web can be a dangerous place for children. Before allowing your children to use the Internet without

supervision draw up a set of rules to be agreed by everyone.

If you're not quite sure where to begin check out the following ideas on what to discuss with your children to teach them how to use the Internet safely:

- Encourage your children to share their Internet experiences with you. Use the Internet with your children;
- Make it quite clear to your children that they must never reveal their address, telephone number or other personal information, such as their school or places where they like to play;
- Teach your children that, on the Internet, the difference between right and wrong is the same as in the real world;
- Teach your children to respect other people online. See that they are aware that the rules of good behaviour do not change merely because they are communicating via a computer;
- Insist that your children have due regard to the online property of others. Explain that making illegal copies of the work of other people - music, video games and other programmes - is considered theft;
- Tell your children they must never meet in person someone that they got to know online. Explain that friends made online may not be who they say they are;
- Teach your children that not everything they read or see online is true. Encourage them to clear up their doubts with you;
- Control your children's online activity with advanced Internet software. The access-restriction controls can help you to filter inappropriate contents, to monitor the sites that your children visit and to discover what they do on such sites.



## News:

### **Telephone Phishing**

Phishing schemes usually use e-mail to direct potential victims to fake Web pages. A new form of phishing has now appeared.



Instead of being directed to a Web page, you may be advised to ring a certain customer-support phone number, through which someone or an audio recording will ask you to provide information such as your account number, identity card number, passwords or other data of a personal nature that could be used to access your account.

Often, the person at the other end of the line will say that your account is going to be closed, or that other problems could occur if you don't answer the questions.


Advice to help prevent telephone phishing:

- View all unsolicited e-mail (and phone calls) with scepticism and avoid clicking on links to Web pages;
- Before phoning, try to identify the telephone indicatives and avoid calling numbers that don't belong you your local network, to prevent costs of long-distance, international or value-added calls;
- Try to determine whether there are real customer-support and other phone numbers by visiting the organisation's Web page. When searching, don't click on any link that appears in an e-mail message. Always write the address in your browser's address bar;
- If you have had any transactions with the company in question, check their invoice or other document to see their real phone numbers and other information. You can also find the customer support numbers of companies that manage credit cards on the back of the cards;
- Keep informed about the most recent identity-theft schemes by means of security newsletters, Web sites managed by institutions involved in online security and other trusted sources;
- Check incoming e-mail messages for signs of phishing attack attempts, such as grammatical errors, suspect Web addresses or other items raising suspicion.



## Basic Security Principles:

### Browser hijacking



Highjacking is a common form of online attack in which the highjackers take control of your computer's Internet browser and alter its

appearance when you are navigating around the Web. If you keep your software up to date, install the most recent security updates and ensure secure conduct when surfing on the Internet you will be doing quite a lot to keep "attackers" at bay.

But if your computer has been highjacked there are several ways to release it from the grasp of the highjackers and to restore your configurations.

How to know if your browser has been highjacked?

Check for the following:

- Your computer's Home Page or other configurations have been altered, including additions of hyperlinks directing you to Web sites you would normally avoid;
- Inability to navigate to certain Web pages such as anti-spyware and security software sites;
- Appearance of a cascade of pup-ups. An apparently endless barrier of ads appears on your monitor;


- Tools bars have been installed or new short cuts added to your Favourites, providing icons and hyperlinks to Web pages you don't want;
- Your computer slows. Malicious software could make your computer slow down.

In the next newsletter we shall provide several suggestions to help restore the configurations of your browser if you are hijacked.



## Configuring and updating software:

### Improve your safety on the Internet and that of your mailbox

An illustration of a lifebuoy with a blue and red striped ring, and a computer monitor with an '@' symbol floating inside it.

Evil-minded hijackers and virus creators can infect your computer, taking advantage of low-security definitions of your e-mail programme and Web

browsing software. They can do so by sending an e-mail with a virus, perhaps in an attachment, or by convincing you to visit a Web site with infected contents.

You can help limit the possibility of becoming a victim of attack by increasing your security definitions.

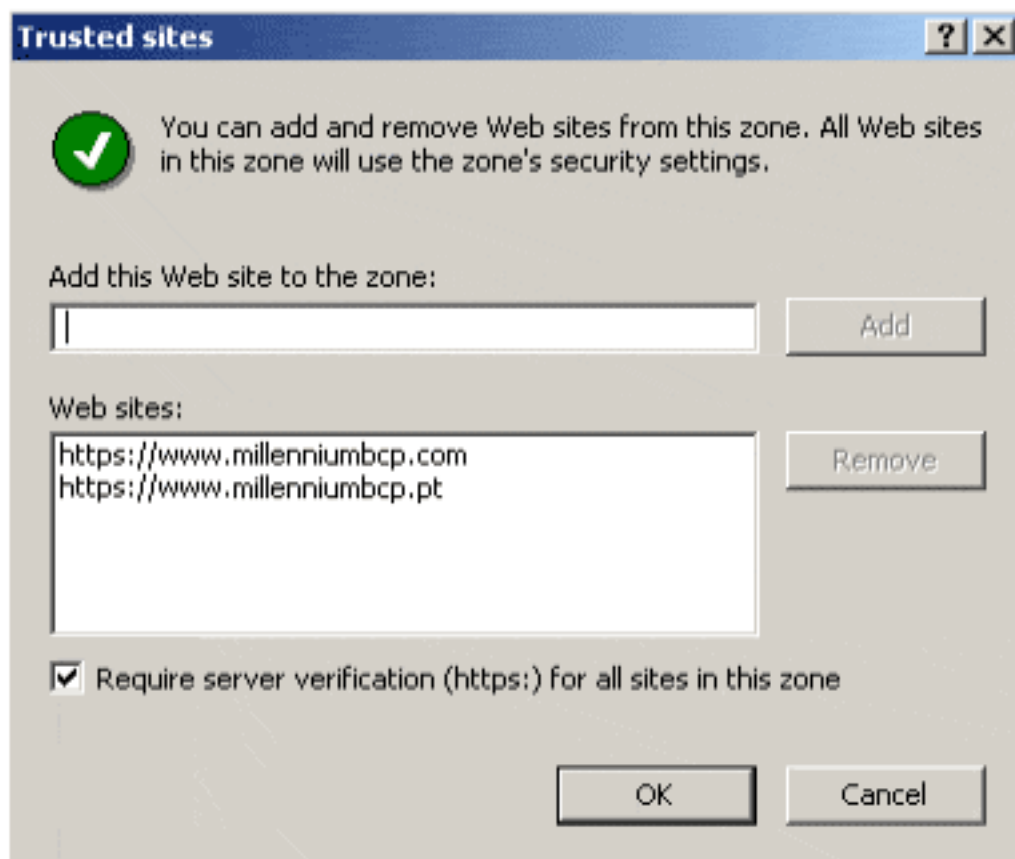
Do so as follows:

#### 1. **Add Web sites your consider safe to the Trusted Sites zone**

To add a Web site to your list of trusted sites:

- In the **Internet Explorer Tools** menu click on **Internet Options**;
- In the **Internet Options** dialogue box, click on the **Security** Tab;
- Click on the **Trusted Sites** icon and click the **Sites** button;
- In the **Trusted Sites** dialogue box write the Web address in the **Add this Web site to** the zone box and click on Add.

This configuration of **Trusted Sites** allows you to restrict the level of confidence just to those sites beginning with https:. To include sites that begin with http:, including the Microsoft Update, clear the **Require server verification (https:) for all sites in this zone** box.



Millennium bcp Site added to the Trusted Sites zone

- Click on **OK**;
- In **Security level for this zone**, move the cursor to **Medium**. This determines that the security level for all the sites of this zone, which you consider trustworthy, is Medium. (If you can't see a cursor, click on **Default Level**, then move the cursor to **Medium**).

## 2. Use plain text to read e-mail messages received

To read text messages in Microsoft Outlook Express:

- In the **Tools** menu of Outlook Express, click on **Options**;
- Click on the **Read** tab;
- Select the **Read all messages in plain text** check box;
- Click on **OK**.

## 3. Activate your browser's Pop-up Blocker

A pop-up blocker prevents small secondary windows from appearing on your monitor when using your browser to visit Web sites. Some Web sites use these small windows to provide useful information, though many pop-up windows contain ads or offensive contents. Malicious hackers may also use pop-up windows disguised as special offers to install malicious code in your computer.

Windows XP SP2 users may take advantage of the Pop-up Blocker provided by Internet Explorer on the **Internet Options Privacy** tab.



"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