

We are back again to share another Year of Security Talk: about the risks to which you may be subject when using your computer to surf the Internet, and about the preventive measures you should use to prevent them.

We trust that all the recommendations made will be more than useful and will lead to changes in behaviour and contribute to an enrichment of your knowledge of information technology.

We are therefore issuing a challenge this month: answer a short quiz to test the knowledge you have acquired.

Highlights:

Phishing activity at Millennium bcp

As has happened with several domestic and foreign banking institutions, Millennium bcp has once again been subject to phishing



activity.

Several customers have received an electronic mail message, reproduced below, inviting them to access a link which, supposedly for security reasons, would redirect them to the Millennium bcp site to confirm their data... >>

News:

A new Trojan Horse has appeared?

The Trojan Horse of mythology seemed to be a gift, though in fact it contained Greek soldiers who took over the city of Troy....>>



Basic Security Principles:

Security Quiz

Test your knowledge. Accept our challenge... >>



Configuring and updating software:

Ways to protect your electronic mail (Part II)

In the wake of our previous Newsletter in which we provided an article on "Protection against unsolicited mail", this month we shall talk about "Virus Protection" when using Outlook Express... >>



Highlights:

Phishing activity at Millennium bcp

As has happened with several domestic and foreign banking institutions, Millennium bcp has once again been subject to phishing activity.

Several customers have received an electronic mail message, reproduced below, inviting them to access a link which, supposedly for security reasons, would redirect them to the Millennium bcp site to confirm their data.

From: Banco Millenniumbcp <seguranca@millenniumbcp.____>

Sent: Sun, 5 Feb 2006 05:02:15

To: <cliente@mail.____.____>

Subject: Recadastramento de Segurança

Caso não consiga visualizar correctamente este e-mail por favor [clique aqui](#)

Mensagem importante, leia com atenção:

Exmo. Senhor(a)

Por determinação do grupo, voltado á segurança de transações online de Portugal, é expresso que todos os clientes do Millenniumbcp deverão recadastrar seus dados bancários imediatamente para que sua conta entre no mais novo sistema anti-fraude de internet banking.

Visando ainda aumentar a sua segurança, o novo sistema já esta incorporado ao sistema anti-fraude e seguindo leis internacionais, mas sua conta so entrará no novo sistema após confirmação dos seus dados, se recadastre agora, clicando aqui www.millenniumbcp.pt

O Millenniumbcp, sempre preocupado com você.

By clicking on these links the customer is led to a page, similar in every way to the Millennium bcp site, the object of which is to collect credentials allowing access to Millennium bcp with a view to possible malicious use.

You can view this page below:

Millennium bcp - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Print Mail

Address <http://www.millenniumbcp.info/> Go Links

Millennium bcp

Particulares | [Empresas](#)
Domingo, 5 de fevereiro

Fiscalidade | Imobiliário | Saúde | Automóveis | Viagens | Lazer

Home Contas Poupança & Investimento Bolsa | Cartões | Crédito | Seguros

English | Registo | e-mail | [Ajuda](#) | [Proteja o seu PC](#) | [Provedor do Cliente](#)

Recadastramento

Caro(a) Cliente,

Preencha os dados com atenção :

Nome:

Bilhete Identidade :

Número Contribuinte:

Telefone/Telemovel:

Confirme os dados abaixo:

Banco: Número da conta:

O seu [Código de Utilizador](#):

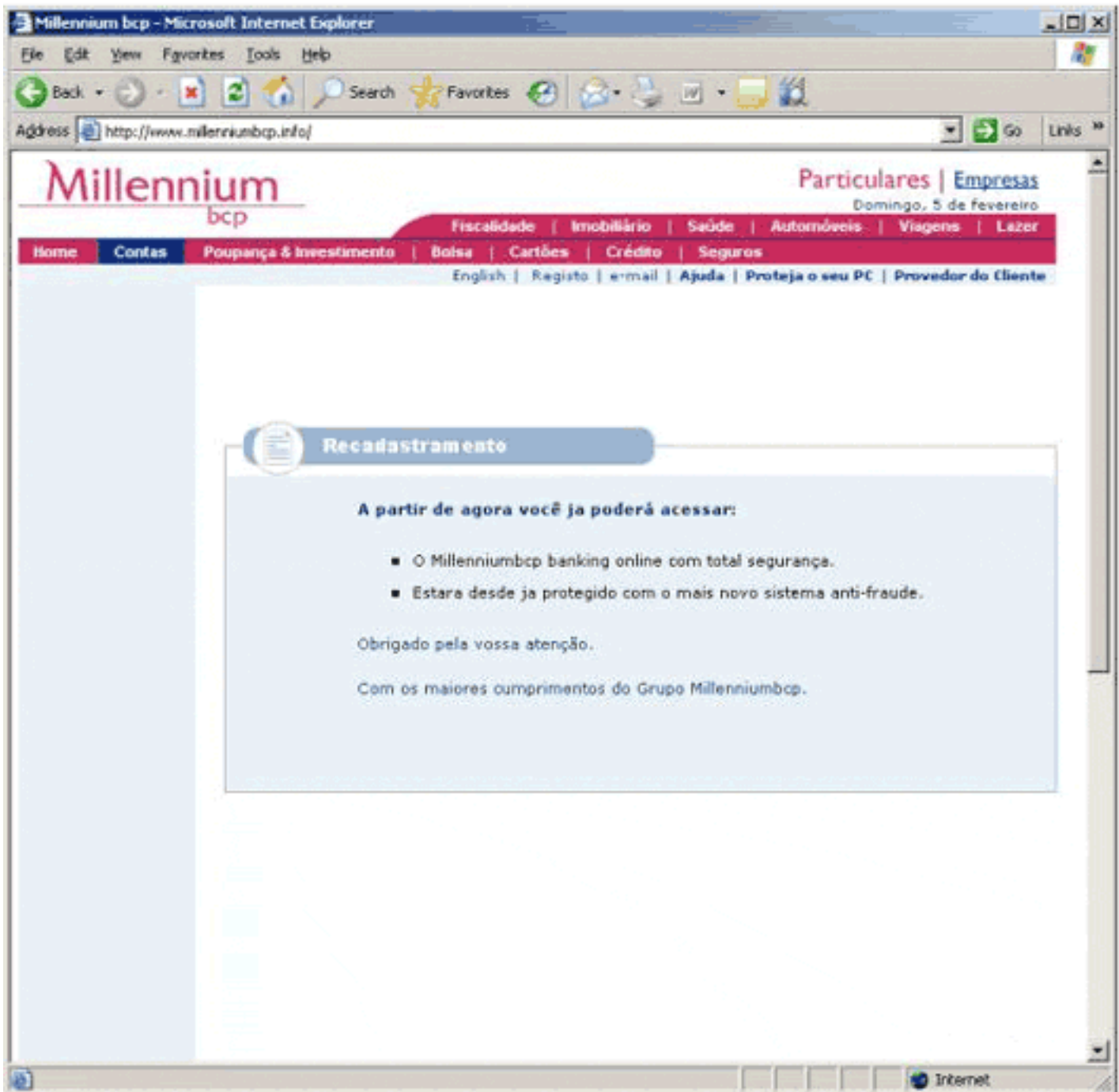
O seu [Acesso Multicanal](#):

O seu [Chave de Confirmação](#):

Confirmo o aqui todos os meus dados.

Enviar

Internet



Despite the many warnings given to our customers by means of newsletters and other warnings on our site to the effect that Millennium bcp **NEVER** sends electronic messages requesting you to introduce home banking access codes or information of a personal or confidential nature, **it could be that some customers may have provided such information.**

Therefore, if by chance you did provide the information requested in the page shown above, please contact us to that we may quickly put the matter right.

We would like to take this opportunity to thank all our customers who called our attention to this case of phishing. We would be grateful if, in any similar case in the future, you would kindly continue to contact us, to inform us of your concerns. **The contribution of all is essential to overcoming situations of this kind.**

Lastly, we would like to point out that, as is obvious, Millennium bcp has no responsibility in this matter, particularly in providing electronic mail addresses. The electronic mail address lists in use are generally obtained by means of spam messages provided by entities that are able, through various means, to obtain electronic mail addresses in the most varied ways, such as:

- Spam – Hoax lists,
- Chain letters – fake friendship and solidarity chains,
- malicious programmes (malware) introduced into computers without protection systems (antivirus, firewall, etc),
- Scams,
- or any fast search using a search engine.

We would once again call the attention of our customers to the care to be taken:

- **Never** provide details of a **personal or confidential** nature in reply to electronic mail messages;
- Always **type in the address of the site** you want to access, **never access through links** (short cuts), even out of mere curiosity.

Contact us if you have any doubt or need any explanation, either by e-mail or telephone
707 50 24 24



News:

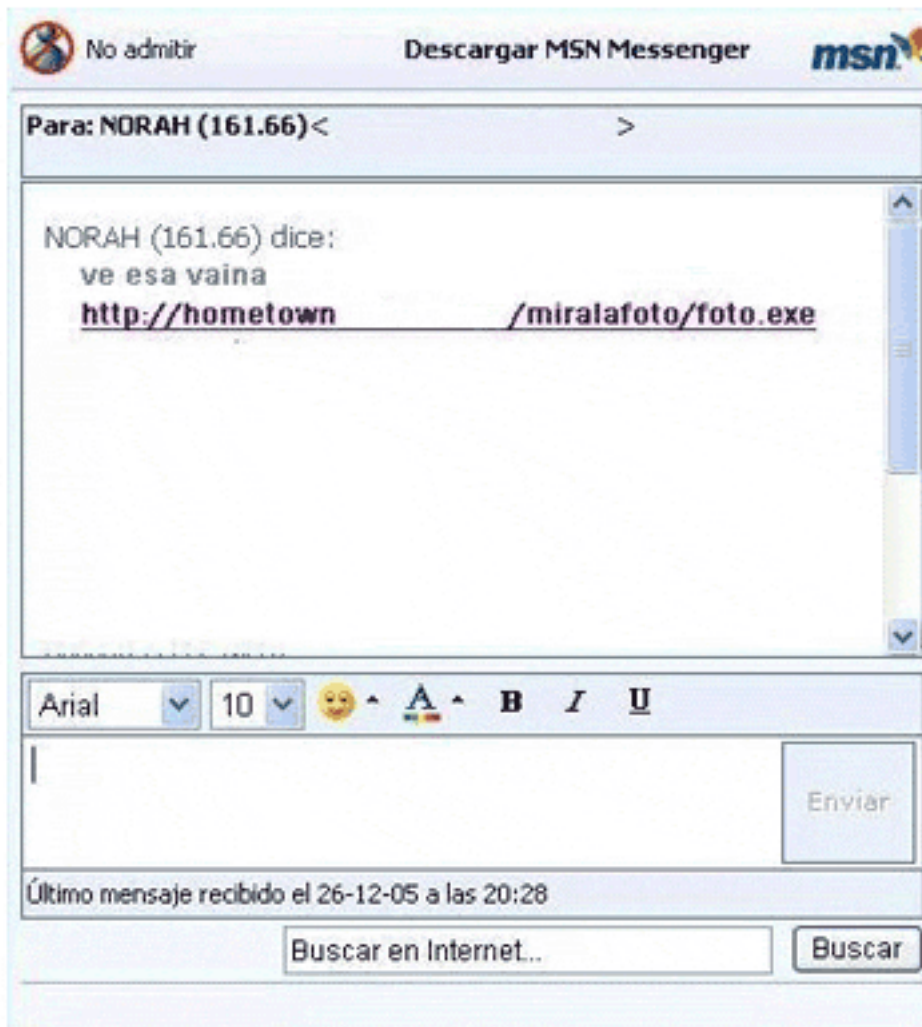
A new Trojan Horse has appeared?

The Trojan Horse of mythology seemed to be a gift, though in fact it contained Greek soldiers who took over the city of Troy. In the same way,

Trojan horses, the modern Trojan horses, are computer programs that appear to be useful software but, in fact, compromise the user's security and cause a lot of damage.

The aim of this new Trojan horse, which spreads via MSN Messenger, is to capture access passwords from users of online banking services of various Latin American countries, particularly in neighbouring Spain.

On receiving a message that appears to come from one of your personal contacts and on clicking on a link that it contains, you will download and execute a Trojan horse known as Nabload.U that will infect your computer with a second Trojan horse, the Banker-BSX.



The above image provides an example of one of these instant messages in which, if you click on the link, the Trojan horse Naload.U will be downloaded and will affect your computer.

Meanwhile, Banker.BSX, the second Trojan waits to capture the login and password if the user visits any one of 10 Spanish online banking sites. The information that is gathered is then forwarded to an e-mail address that the hacker can alter as often as he likes.

Contrary to past practice, this new Trojan is able to capture the logins and passwords without using the traditional keylogger, which means that the banks that use what are known as virtual keyboards to prevent this kind of malicious activity are no longer protected.

Signs of this Spyware activity have been found in Chile, Israel, Peru and Argentina. No similar activity has been encountered in Portugal.

To check whether you have been infected with this Trojan we suggest that you update your Antivirus and Anti-Spyware software and then scan you computer.



Security Quiz

Test your knowledge.
Accept our challenge...

1. How does a virus infect your computer?

- a. Executing an unknown program on a floppy disk or even on a CD-ROM;
- b. Installing documents of doubtful origin on opening Word or Excel documents, etc;
- c. Opening Word or Excel documents, etc., as well as documents attached to e-mail messages;
- d. All the above possibilities.

2. Which files are more dangerous?

- a. those ending: .jpg, .gif, .mp3;
- b. those ending: .exe, .com, .bat or .vbs.

3. Keyloggers – What are they?

- a. Antivirus software;
- b. Spyware-type programs;
- c. Entertainment programs.

4. What is a Firewall?

- a. A computer lining to protect it from fire;
- b. A personal Internet access code;
- c. Software or equipment that helps protect your computer from malicious attacks.

5. After antivirus software is installed my computer is fully protected?

- a. True;
- b. False.

6. You can be infected with Spyware:

- a. By downloading programs from unknown sources;
- b. By downloading music, films, games or other software from file sharing programs on the Internet;
- c. Navigating around the Internet visiting sites of doubtful origin;
- d. All the foregoing possibilities.

7. What should I do after installing antivirus software?

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

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

- a. Install all the security updates provided by the supplier;
- b. Install antivirus software and update it regularly;
- c. Install an anti-spyware programme and update it regularly;
- d. All the foregoing.

The right answers will be provided in the next Newsletter.



Configuring and updating software:

Ways of protecting your e-mail (Part II)



In the wake of our previous Newsletter in which we provided an article on "Protection against unsolicited mail", this month we shall talk about "Virus Protection" when using Outlook Express. Under Windows XP SP2, Outlook Express has been altered and improvements introduced at security level. These new definitions provide better help in preventing the viewing of offensive contents of e-mail messages, reducing the quantity of unsolicited mail (spam) and reducing the reception of hazardous contents through an e-mail message.

To view or alter the security functions in Outlook Express:

1. In Outlook Express, go to **Tools**;
2. Click on **Options**;
3. Click on the **Security** tab.

Virus Protection Definitions in Outlook Express

Your computer may become infected with virus or worms when you navigate on the Web, download files or open e-mail attachments. Any e-mail message, even though apparently inoffensive, may damage your personal information or even your computer. Outlook Express now has definitions that can help prevent virus and worms in several ways.

- Select the Internet Explorer security zone to use;
- Warn me when other applications try to send mail as me;
- Do not allow attachments to be saved or opened that could potentially be a virus.





"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