

In June, on the 21st or close to it, the Sun reaches its furthest distance, in terms of latitude, from the equator in its trajectory through the sky.

It is the Summer Solstice, the beginning of Summer in the Northern hemisphere.

And normally associated with the Summer are holidays.

This is why we thought it was appropriate to publish an article in "Em Destaque" on "Fraud in Self-Banking", at a time when this seems to take place the most.

And also so that fraud involved in providing your personal and confidential information won't be something totally new to you, we would once again warn you about the care you should take concerning Phishing. Follow our advice.

And while we are at it, have a great Summer!

Highlights:

Fraud in Self Banking

As Summer draws near people tend to use Self Banking equipment even more. There is also the possibility of an increase in the number of related accounts of fraud. Such



fraud occurs through the electronic theft of card data by the use of card readers inserted into the legitimate equipment.

So, there is a real possibility of a disguised card reader being inserted into an ATM, a Cheque Dispensing Machine or even in the Access to the Self-Banking machine area which will gather the data from the magnetic strips which are passed through them... >>

News:

Tips to avoid Phishing

1 - Take special care with unsolicited e-mail messages, even if they appear to be from a trustworthy source...

>>

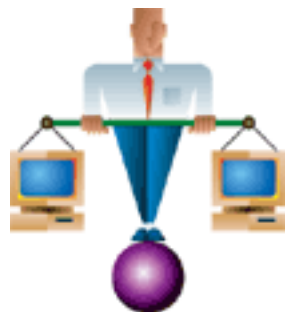


Basic Security Principles:

Restoring a manipulated browser

Today we will give you some suggestions in order to help you restore your browser configurations if these have been manipulated... >>





Configuring and updating software:

Improve your safety on the Internet and that of your mailbox

Before receiving Windows Update software or being able to obtain programs from the Transfer Centre, Microsoft will ask you to validate your copy of Windows ... >>

Highlights:

Fraud in Self Banking

As Summer draws near people tend to use Self Banking equipment even more. There is also the possibility of an increase in the number of related accounts of fraud. Such fraud occurs through the electronic theft of card data by the use of card readers inserted into the legitimate equipment.

So, there is a real possibility of a disguised card reader being inserted into an ATM, a Cheque Dispensing Machine or even in the Access to the Self-Banking machine area which will gather the data from the magnetic strips which are passed through them.

You should know the main steps to take:

RECOMMENDATIONS

It is therefore recommended that you take the following things into account:

- Check if there are foreign objects in the entrance to the card reader;
- Check if there are signs of glue around the card reader slot;
- Check if there are foreign objects in the upper panels of the ATM or Cheque Dispenser;
- Check if the panels have been violated, altered or if there are signs of glue on these panels.

EMERGENCY CONTACTS

If you detect any of the situations mentioned we suggest that you inform the Millennium bcp by calling one of the following numbers:

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

You may also immediately contact the SIBS Network Management by dialling **217 813 020**.

PHOTOS

Below are some photographs showing examples of a false device (Photo no. 1) and also traces of glue

on the card insert slot (Photo no. 2):



Photo no. 1



Photo no. 2



News:



Tips to avoid Phishing

1 - Take special care with unsolicited e-mail messages, even if they appear to be from a trustworthy source;

2 - Do not trust accesses to sites using links included in e-mail messages. The alternative of performing "Copy" and "Paste" on the link into the browser is also not safe;

Instead open a new browser window and write the full address of the site you wish to access.

Any message sent by the Millennium bcp via e-mail never contains links and neither do they request access codes or other confidential information. Whenever you wish to access the Millennium bcp, write the full address (www.millenniumbcp.pt) in the browser.

3 - Do not trust non-personalised messages which do not mention your name and which begin with: "Dear Sir", "Dear customer", etc.;

4 - Question the reason why the Company is contacting you;
If you are in any doubt contact it by telephone or Access the respective site directly.

5 - Do not click on attachments to e-mail messages, these could contain viruses or Spyware - Keyloggers which could get and record anything and everything you write, such as Passwords or Credit Card numbers;

6 - Before entering private or confidential information, always check is the address of the page you are

accessing begins with **https://** ("s" means "safe") and if the lock is visible in the lower corner of the browser;

7 - If you see the symbol "@" in the middle of a site address this may mean that the site is false;


8 - Always keep your computer's software up-to-date, never forgetting your Antivirus' periodic updates.

Keep your eyes open!



Basic Security Principles:

Restoring a manipulated browser



In the last Safety Newsletter, when we spoke of "browser manipulation", you were told how to notice the signs of this type of online attack. Today we will give you some suggestions in order to help you restore your browser configurations if these have been manipulated.

- **Prevent successive pop-up windows**

If an apparently endless number of pop-ups appear on your screen, and in order to stop this, in Microsoft Windows XP or Windows 2000, while you use Internet Explorer, you should:

1. Press **CTRL+ALT+DEL**, click on the Windows **Task Manager** and then on the **Processes** separator;
2. Click on **IEXPLORE.EXE** and then on the **End process** button.

This closes all the instances of Internet Explorer. Then you can re-open the program to continue surfing normally. In order to help you prevent future attacks you should also activate a pop-up blocker.

- **To activate the pop-up blocker in Internet Explorer:**

1. In the Tools menu, click on Internet Options and then on the Privacy separator;
2. In the Pop-up Blocker section at the bottom, click on the Block Pop-ups box to activate it.

- **If other effects of a browser manipulation continue then try the following:**

1. Install software to prevent browser manipulation. Many browser manipulation programs can be identified and removed by transferring, installing and executing these programs;
2. Execute the malicious software removal tool. This can detect some types of manipulation software, but not all.

If you are using Internet Explorer and your initial page has been altered, you can reconfigure it by yourself.

How?

- In the **Tools** menu, click on **Internet Options** and then on the **General separator**;
- In the **Home Page** box, write the Web address you want to see in the Address Bar, or click on the button **Use Default** to restore the original manufacturer's configurations;
- Click on **OK**.



Configuring and updating software:

Advantages of using Windows Genuine Advantage software



Before receiving Windows Update software or being able to obtain programs from the Transfer Centre, Microsoft will ask you to validate your copy of

Windows XP. Updates are only available to users who confirm that their Microsoft software is genuine and not a pirate copy.

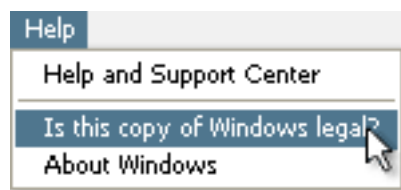
(To help customers who need more time to move over to genuine Windows software, Microsoft will continue to offer security updates through Windows Automatic Updates, with or without validation of Windows Genuine Advantage).

By only using genuine Microsoft software, you can be certain that your software is legitimate and has the full support of Microsoft.

Genuine Microsoft software is licensed software, certified as authentic, published and supported by Microsoft. The advantages in using genuine Windows software include:

- Faster Access to updates
- Greater reliability
- A more rewarding experience
- Access to special offers

Microsoft offers an online tool which allows you to confirm that your copy of Windows is genuine. The validation process is short and simple and, once concluded, it means that in the future you can access genuine transfers of Windows more quickly. After a successful validation, a Microsoft Windows Transfer Code will be stored in your system for future use.



You can validate your copy of Windows by visiting the page <http://www.microsoft.com/portugal/conformidade> and clicking on the link of the image which says "**Ask for genuine Microsoft software**". Then click on **Windows Validation**.



"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