At the end of this chapter you will be able to:

1] Configure user levels and passwords.

2] Recognize the necessary aspects for PC security and home networks.

3] Keep your system updated and protect it against the threats of spyware and viruses.

4] Protect and take care of your PC’s physical resources.

5] Know the ways to protect data and the existing programs in the PC or portable devices.

In this chapter you will find:

- How to configure and select the security passwords in Windows?
- What security measures must be taken when you share resources in a network?
- What are the ways to protect the physical security of the resources?
- How to protect data and programs stored in your PC or other portable devices?

PC SECURITY
INTRODUCTION TO THE CHAPTER

You have surely heard about “PC security”: in companies as well as in other environments, several people are dealing with this issue and worried about it. PC security involves a challenge: to protect the devices and assure the integrity of the information in the systems. To do so, several strategies are implemented, whose aim is to protect both PCs and users and they translate into a set of "security measures". Although it is almost impossible to obtain a 100% secure system, it is essential to know the different issues that can affect our PCs, and reduce the security risks to a minimum level.

So in this chapter, we will discuss this topic which, as implied by the above mentioned statements, is highly important: **PC security**. This comprises different aspects that need to be considered, as a member of your school’s technical support team. First, you will learn how to establish secure passwords for the different types and levels of users. You will also learn about the ways to share resources securely, promoting network protection. The aim of all these issues is that you can learn more about the security tools in the operating system, and how to properly implement them. Pay attention and start taking notes to organize the security measures suitable for your school...
CONCEPTUAL MAP OF THE CHAPTER

- **User Accounts**
  - Assigning and changing passwords in Windows
- **Networks**
  - Establish passwords
  - Share resources securely
- **Software**
  - Preventive practices. Windows Update
  - Set up Firewall options from the Activity Center, Install Antivirus, Update virus definitions
- **Hardware**
  - Bitlocker Data Protection
  - Hardware electrical security, using voltage stabilizers
- **Physical Security**
  - Maintenance, Creation of Inventories

58. Use shared folders in Windows Live Messenger
How to assign passwords in Windows 7

In chapter 4 you have learned, as part of the technical support team, the importance of creating user accounts in order to differentiate the access to the Administrator and the general users options. This is specially important in the school where one PC is used both by students and teachers: here, you will learn to set up user accounts in a way that students can access certain information and teachers other, but in the same PC.

Let’s start with the Users. Although we must pay special attention to the security measures in the Administrator user, as it is the one with credentials to make changes in the system, we cannot forget these issues in the standard users: in this type of accounts it is also important to establish a Windows 7 password.

Did you know…?

...that sending unwanted email, called SPAM, consumes up to 30 thousand million kilowatt per hour around the world?

Password

Password:
A set of characters created by the users that enable them to safely interact with the PC.
In order to assign a password to a user account, follow these steps:

01 Type “password” in the Start menu. One of the options is Change Windows Password. When selecting this option, the screen of the user you are using will appear.

02 If the user has not created a password, you must select the option: Create a password for the account.

03 A second screen will show the name and type of user and then will prompt you to enter a new password twice.

04 Once the information is complete press the Create password button, and you can start to work as a user with a security password.

We recommend to assign passwords both for the Administrator and the standard user.
Steps to change an existing password

If you want to change an existing password, follow these steps:

01 Type “password” in the Start menu
02 Select Change Windows Password and then choose the Change Windows Password option in the Make changes in the user account window.

Why do you have to enter the password twice?

In computing, entering new passwords twice is a usual practice and prevents any involuntary error when typing. Windows 7 also asks for a password hint, this is, a clue that makes remembering it easier if by any reason we forget it.

It is important that the hint does not include the password itself or any specific information that may give it away. In this way, you will prevent unauthorized users from accessing your PC, by simply looking at the hint or key word that you have selected.

Passwort Hint

It is the hint that makes it simple for the users to remember the password in case they forget it.

Tip!

Although it is really important that the PC uses security barriers, it also important to implement it in an efficient way.

If the user and passwords can be reached by anyone that is near the PCs, the security measures implemented are useless.
03 In the next screen, select the **Change password** option.

04 Windows needs to confirm that you are the **active user**, so it will ask for the current Windows password. Enter the **new password twice**, and then the password **Hint** as you have done when assigning a new password.

05 Finally, press the **Change password** button. Ready! Your user will have the new password enabled.

---

**How to select a secure password?**

Secure passwords are those having at least 8 (eight) characters including upper case letters, lower case letters, and numbers. You must avoid the usual passwords, such as 1234567 or qwerty, as they are obvious sequences whether because they are a logical series or a continuous keyboard series. You must also remember not to use passwords that are easy to discover, such as your birth date, your home address, or your ID number. Although this may seem silly, this is something users usually do, and are practices that must be avoided to get a greater security.
How to assign a password to the network?

In the previous chapter, you have learned to set up a network for your home or even your school. But it is important to add some extra knowledge: how to assign a password to your network to protect it and make it more secure.

Here, you will learn to set up a password for the moment you install a wireless router:

01 Type “Network and Shared Resources Center” in the Windows 7 Start menu and access by clicking on it.

02 Click on Configure a new connection or network.

03 Then, select the Configure a new network option and click on Next.

04 Follow the wizard’s steps that will request information, such as the name of the network and a security password. If your router allows it, the wizard will use the Wi-Fi Access protected (WPA or WPA2) default security option. We recommend to use WPA2 because offers a greater security than the WPA security or Wire Equivalent Privacy (WEP) option.
Share resources securely

When you are working over the network, another important topic to consider is the shared resources security: printers, devices or folders, and network drives. Regarding the network drives, it is important to set the authorizations correctly so that only authorized users can access them.

Windows 7 takes advantage of the new technology called: HomeGroup. So if you have your network setup in this way, you will be able to maximize its use by selecting some security options.

If you want to safely share resources, you must place the mouse on the folder you want to share and press the right button. A series of options will appear, and you will find Share with, there you can select between: None, Home Group (read), Home Group (read and write), and Specific Users.

If you have HomeGroup set up in your network, a simple way to share resources with the members of the Group is to use some of the HomeGroup read or write options.

If you want to share resources with a specific group of users, simply select the Specific User option. Once there, write the user you want to share the resource with and then establish the authorization level: Read only or Read and Write.

If you have any doubts regarding HomeGroup configuration, return to the specific chapter about networks.
from a specific user, just repeat the operation but this time select the **Remove** option in the **authorization levels**. From that moment, **the user will disappear from the list and will no longer have access to the shared resource.**

---

**Enjoy for a while and train yourself!**

Read the descriptions of the characters and join them to the type of user account that best suits each one.

- **Mariel**
  - Is a fourth grade student. She just uses her PC to do the homework sent by her teacher.

- **Alexis**
  - His hobby is painting with watercolors, but he is researching about new ways of digital art. He has been a member of the technical support team for over a year.

- **Laura**
  - She loves literature. She teaches at school and sometimes prepares teaching resources in the PC.

- **John**
  - He teaches Physical Education at school. Sometimes, he goes to the computing lab to check his email account before leaving.

- **James**
  - He teaches IT and collaborates with the school’s help desk explaining the students the technical knowledge they must know.

---

**Standard User Account**
- [It is used for usual tasks]

**Administrator**
- [Has credentials that provide the maximum control over the PC]

**Guest Account**
- [Mainly used for people that temporarily need the PC]
IMPORTANCE OF KEEPING SOFTWARE UPDATED

Other aspect of PC security refers specifically to the software. To make sure that the software you use in your PC has the necessary security levels, you must periodically update it.

Windows 7 provides the tool necessary to check it: by simply accessing the Activity Center and selecting “Windows Update”, you will find the proper information regarding recommended updates to keep the operating system updated and protected.

How to verify the software security?

1. Go to the Start menu and type Activity Center.

2. Once there, you will see the alerts: if Windows Update is disabled or wrongly set-up, a message will inform you within the Security tab.

3. In this case, press the Change configuration button. A screen with the recommended option for Windows Update will appear.

Also, from the Activity Center, is is important to correctly set up the Windows Firewall and the Antivirus you have installed: two key tools related to PC security.

Remember: it is important that all these elements are properly updated to ensure a good operation.

Return to chapter 6 and review the security configuration through the Activity Center.
PHYSICAL SECURITY OF THE RESOURCES

Also protect the Hardware!

Another important topic of the PC security refers to the physical resources.

If your network includes a server or servers that provide the services and store the information, that are accessed by the other PCs, they must be physically protected in a secured location.

One risk may be that someone uses the PC that functions as network server, in order to attack it or simply turn it off affecting all the network users.

Ideally, servers should be in their own environment, locked and properly refrigerated, but if this is not possible, you must try to protect at least the physical integrity, whether by storing them in secured racks or preventing access to them.

In addition, must pay attention to issues related to Electrical Security.

Although today’s devices are prepared for high and low voltage changes so frequent in the power lines, it is important that you use voltage stabilizers in order to minimize the impact in your devices.

If you are interested in having a continuous operation, you need a UPS, Uninterruptible Power System. The UPS is an electrical device that has a battery. When the power is interrupted, the device starts to work and gives your PC some time be properly turned off. Remember that if the PC is not properly turned off, parts of the hard drive may be damaged.
A task for the technical support team: make an inventory of the devices

It is important to make an inventory of the devices at school. A good idea may be to use numbers to identify each component, keyboards, mouses, etc.; in this way you can control the hardware. So when you need to verify the condition of the devices you can use the index created. In addition, when you list the devices, you can use them as reference when they need technical support, as well as keeping a record, such as a whitepaper where all the changes, errors, and repairs are stated.

Depending on the size and the complexity of the UPS, you will have more or less time, after the power interruption. This period of time is technically called “ride-over capacity”. The greater ride-over capacity level, the more time your PC will be on during a power interruption.

Ride-over capacity
A device’s functioning capacity, without being connected to a direct power source.
SECURITY TOOLS FOR DATA PROTECTION

Meet Bitlocker

When talking about the PC security, we need to mention the new tools that enable you to protect the most valuable element in your PC: the information.

**Bitlocker** is a technology that allows to encrypt the hard drive, so if a desktop PC or laptop is lost or damaged, and its hard drive is connected to another PC, the information remains protected.

**How does this work?** Some years ago, hardware manufacturers incorporated a “security chip” called **Trusted Platform Module (TPM)** to their PCs.

**Encrypt**

An action intended to protect, encode, or enclose information so it can only be read with a password.
Today, when you install Windows 7 in a PC, the installer generates a 100-MB partition (or 300 MB if it is 64-bit Windows) where all startup files are located. When the PC is turned on, this partition will realize that the PC’s drive is encrypted and will start the process. The startup partition will request the PC’s **TPM** the code to decrypt the hard drive and Windows 7 will start as usual.

The operating system use will be exactly the same, with no delays when performing the usual tasks.

If that person realizing this decides to set the drive as main drive (**bootable**), it will initiate the Windows 7 startup process, but at some time, the password for the TPM chip will be requested. If it is not obtained, a message will appear on the screen requesting the password, that the person who found the PC will not have.

**Now, what happens if your PC is damaged and you have to use the drive in another PC?** It will happen what we

**Bootable**

It refers to the part of a drive where information necessary for the operating system startup is kept.

**In case you lose your PC, whoever finds it will not be able to access the information because they will not have the password**... Assuming that the person decides to remove the hard drive and connect it to another PC, as the Windows 7 protected Drive has not been turned on as main drive, it will remain off, encrypted, and the information protected.
explained before: you will not be able to access the data as the system can no longer request the TPM password. What you have to do is to insert the Windows 7 installation DVD and start the PC. At this moment, the installation program will realize that there is a drive protected by Bitlocker and will request the password.

In addition, one of the improvements in Windows 7 is related to the ability to extend the Bitlocker Drive Encryption functionality in order to protect also the portable storage devices: pendrive, external hard drive, etc... Using the same concepts as its older brother, this feature allows you to encrypt the information in those portable devices.

In order to encrypt a removable device, you have to connect it to the PC. Then, you must access PC in the Start menu. Right click on the device and look for the Enable Bitlocker option...

Once this option is selected, the screen corresponding to this process will appear. While it is starting, Windows 7 will verify that the minimum requirements to encrypt the device are met, and two options will appear:

- Use a password to lock the drive; or
- Use the smart card to block the drive.

If you choose the most common option, to use a password, select the corresponding checkbox to type it. For security reasons, the system will ask you to repeat the password and click Next.

In the second and last screen “How do you want to store the recovery token?”, you will find two options: the first one is Save the token in a location you select, and the second one is to print it.
Once you select **any** of these options, and after clicking Next, the registration process will start (its duration will be proportional to the space of the device to be protected).

As seen before, you can protect the hard drive and the portable drives and USB devices that you use without any problem.

Some fun to learn!

Put some of the concepts you have studied in this chapter into the following chart.

Use the letters as a guide...
How to verify your PC's security in Windows 7?

There are many aspects to be taken into account to keep your PC secured. As you have seen, Windows 7 helps you with its different tools. In order to make sure that you are using all these features and verify that your PC has the maximum security level, the following icons will guide you through the tools provided by the operating system to get a secured environment. If you want to know more about any of them, visit:

Green tip

Security is a value and a goal of every human being: as individual persons, as families and in the community, people like to feel protected. Security, in this way, implies several aspects that range from feelings to technical and material conditions of everyday life. In the same way as we learn to promote security in our PCs, it is important to always consider environmental security. It is an issue that we always have to bear in mind, no matter the activity we are carrying out. Many times, human beings habits and practices harm the environment, and even if they are small, they negatively affect the natural surroundings. Experts say that human beings would need more than two planets to renew the resources they are consuming. These figures make us realize that the Environment is in danger and needs our commitment to alleviate the situation. Therefore, we need to add up our contributions in order to make a change that promotes "Environmental Safety". By adopting a "green attitude" from school, we will be contributing our share to this cultural change movement related to the protection of the planet.
Complete the following exercises to review your knowledge about PC security.

A. Define in your own words what SECURITY is. Include in your definition the different aspects that must be taken into account when promoting a secured PC environment.

____________________________________________________________________________________________________________________________________________________________
____________________________________________________________________________________________________________________________________________________________

B. Check the user accounts of the different PCs in your school’s lab and verify which of them have passwords. Also, check the type of user account.

Based on the information gathered, make a strategic plan to organize the user accounts of the different PCs.

Use the following chart as model for a better organization.

<table>
<thead>
<tr>
<th>User Name</th>
<th>PC1</th>
<th>User 1</th>
<th>User 2</th>
<th>User 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does it have a password?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C. Make a small research about the electrical security condition in your school and prepare a prospective report with tips for improving the general condition.

You can use the following items as guidelines:
- How many electrical outlets are there in the Computing lab?
- Watch the condition of the wires: look if they are tangled, if they have stripped wires, etc.
- Are there voltage stabilizers in your school?
- Find out about the behavior of the power lines in your area: Are tension variations usual?

D. Use the chapter’s conceptual map and complete it by breaking down the knowledge acquired in this chapter.
Self-assessment
Check what you’ve learned through the following questionnaire

1. For what type of user is advisable to assign passwords?
   a. For the standard user that performs usual tasks in the PC.
   b. For the Administrator who has the credentials to make changes in the PC.
   c. Both users

2. What is the minimum amount of characters for a password to be secure?
   a. At least 6 (six)
   b. At least 8 (eight)
   c. At least 4 (four)

3. With the HomeGroup feature, resources can only be shared with the read option.
   a. True
   b. False

4. Which acronym is used to call the “security chip” of a PC?
   a. PMT
   b. TMP
   c. TPM

5. What is the component that allows your PC to continue working even when there is a power interruption called?
   a. UPS
   b. TPM
   c. USM

6. How is the security tool that allows to encrypt a drive to protect information called?
   a. Firewall
   b. Winsecurity
   c. Bitlocker

7. What does “ride-over capacity” mean?
   a. A device’s capacity to continue performing tasks even when the user is not there.
   b. A device’s functioning ability, without being connected to a direct power supply.
   c. The pre-active function of Windows 7 to keep the PC secured.

8. The Bitlocker tool can be used both for the hard drive and for portable devices.
   a. True
   b. False

9. Through which Windows 7 tool can you access Windows Update in order to verify permanent software update?
   a. Windows Security
   b. Activity Center
   c. Desktop

10. Which of the following Windows 7 tools promote PC security?
    a. Windows Defender and Windows Firewall
    b. User Account Control and Microsoft Office
    c. Both are correct