



Em destaque

Trojan Horses - "Cavalos de Tróia"

Mais +



Princípios básicos de segurança

A Segurança no Windows 7

Mais +

[English version](#)



Token Reader

Códigos de Autorização, para confirmação das suas operações na internet, em Portugal ou no estrangeiro.



Visite a área de Shopping em www.millenniumbcp.pt



Em destaque

Trojan Horses - "Cavalos de Tróia"



Um pouco de história

A expressão "Cavalo de Tróia" (*Trojan Horse*) surgiu na mitologia grega. Reza a história que os Troianos foram presenteados pelos Gregos com um grande cavalo de madeira para promover a paz, mas, no seu interior, escondia-se um grupo de soldados gregos que esperaram pela noite para abrir os portões da cidade e tomarem Tróia.

Os "Cavalos de Tróia" modernos, que passaremos a designar por *Trojans*, são programas de código malicioso que executam acções inesperadas e não autorizadas, causam prejuízos, comportamentos inesperados e comprometem a segurança dos sistemas, abrindo uma porta escondida. Este tipo de programas permite:

- **Roubar credenciais** do utilizador (*passwords*, códigos, etc);
- **Roubar dados** pessoais armazenados no equipamento;
- **Copiar dados** (documentos, ficheiros, etc);
- Criar, do interior da sua rede, uma **quebra na segurança** e, dessa forma, autorizar o acesso às partes protegidas da rede a partir do exterior ou executar qualquer outra acção prejudicial.

Os *Trojans* aparecem muitas vezes disfarçados ("escondidos") de outro *software*, comprometendo a segurança dos computadores e, conseqüentemente, a confidencialidade, integridade e disponibilidade da informação aí residente ou que o utilizador acede através da máquina infectada.

Como se instalam

Estes *Trojans* instalam-se nos computadores quase sempre através de uma acção que o utilizador desenvolve:

1. Ou recebe um email sugestivo que contém um programa anexo;
2. Ou acede a alguns sites e, por via do clique num determinado *link* descarrega e executa um *software* específico;
3. Ou instala um CD/DVD algumas vezes fornecidos por terceiros, que contém *software* não aconselhável.

Em cada uma destas situações poderá estar a proceder à instalação do tal programa malicioso.

Como se "abatem"

Algumas acções de protecção do computador evitam certos efeitos provocados pelo código malicioso, nomeadamente:

1. A utilização e permanente actualização de antivírus, *antispyware* e dos *patches* e *fixes* de segurança dos vários fornecedores de *software*;
2. A utilização de uma *firewall*;
3. A configuração correcta dos equipamentos de acesso à Internet, etc.

Mas os meios tecnológicos só por si não chegam

Tudo isto pode ser insuficiente se o próprio utilizador tomar determinadas acções que ultrapassam todas as protecções que pôs em prática, algumas vezes associadas a investimentos significativos. Quando um utilizador:

1. Toma a iniciativa de fornecer as credenciais ou códigos pessoais a terceiros e estes as utilizam indevidamente;
2. Abre um email e o seu anexo, apenas por curiosidade, sem confirmar antecipadamente a origem e o assunto do mesmo;
3. Acede a determinados sites sugestivos e por via deles efectua o *download* de determinado *software*;
4. Instala *software* do qual não conhece a proveniência;

não há segurança que baste para ultrapassar estas situações.

Daqui poderemos concluir que: **a Segurança começa em nós próprios e de nós depende em grande parte.**

Um exemplo do quotidiano, quando protegemos a nossa casa com tudo o que há de mais sofisticado mas, se alguém, em quem não confiamos, tem acesso à chave da mesma, talvez porque nós próprios a demos ou emprestámos, nesse caso, de nada valeu todo o investimento que efectuámos em segurança. O mesmo princípio aplica-se aos computadores e à utilização que fazemos deles.

Em conclusão: os *Trojan Horses* são *softwares* maliciosos que podem ter efeitos nefastos se instalados nos nossos computadores. Mas, como quase tudo, também se abatem desde que tomemos todos os cuidados necessários.

Proteja o seu computador. Depende muito de si!

Consulte as nossas Newsletters e outros temas de Segurança em www.millenniumbcp.pt.

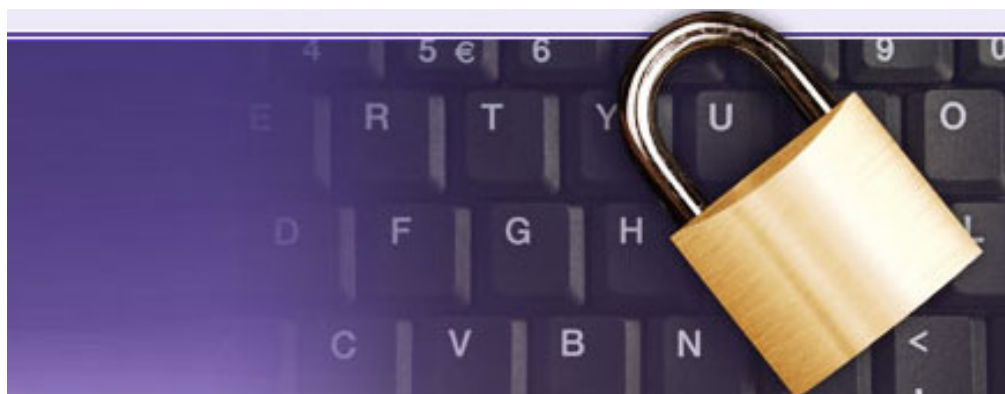
Fonte: millenniumbcp.pt

Topo 



Princípios básicos de segurança

A Segurança no Windows 7



O Windows 7 traz novas possibilidades. Este sistema operativo, além de permitir um PC mais simples e mais rápido, foi pensado tendo a segurança em primeiro plano.

A segurança é, sem qualquer dúvida, um tema muito abrangente. Pode ser simples ou complicado, mais ou menos interessante, mas esperamos, com este texto, mostrar o que se pode e deve esperar relacionado com a segurança no Windows 7, de forma interessante a qualquer utilizador das novas tecnologias, em especial o utilizador particular.

O ponto agregador da segurança no Windows 7: o *ActionCenter*

Cansado das janelas de pop-up? O *ActionCenter* ajuda-o a decidir que alertas o Windows 7 irá ver e quais os que nunca irão aparecer.

É no *ActionCenter* que estão os principais temas de segurança do Windows 7.

Conforme se pode ver na figura 1, no *ActionCenter* encontramos as questões relativas à segurança mas também à manutenção do computador.

Se o Windows 7 requer a sua atenção, é através do *ActionCenter* que essa comunicação irá aparecer.

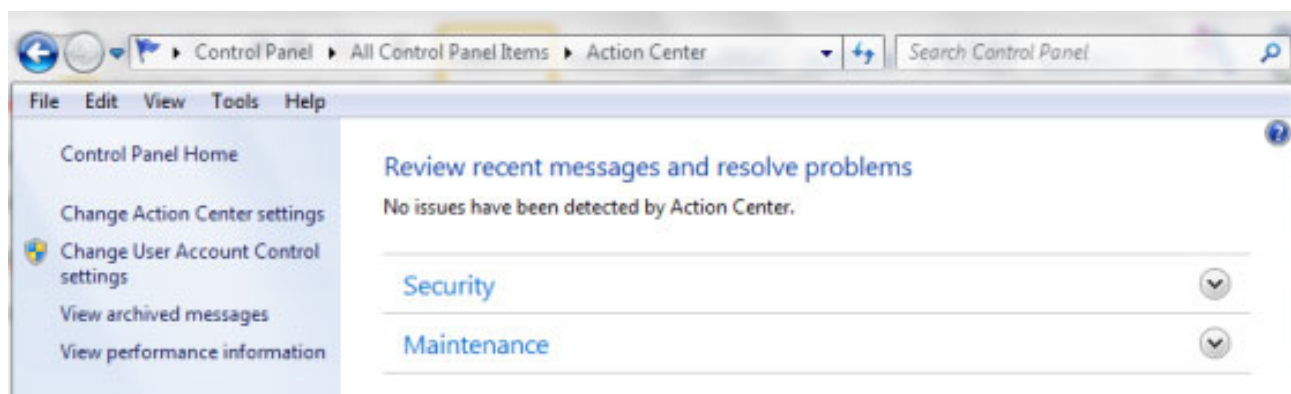



Figura 1: As opções no *ActionCenter*

É aqui que se encontram os alertas e as acções a tomar que ajudam a manter o PC seguro e a funcionar da forma desejada. Se um *item* no *ActionCenter* está marcado a vermelho como Importante, então deveremos ter em atenção esse ponto o mais rápido que nos for possível porque há algo que é fundamental ser resolvido. Como exemplo, poderemos referir um programa antivírus que esteja desactualizado e que por isso mesmo é urgente a sua actualização. Se o alerta for amarelo, quer dizer que teremos tarefas de manutenção que são necessárias ter em consideração, como por exemplo, cópias de segurança.

Existindo mensagens provenientes do *ActionCenter*, elas aparecem no canto inferior direito (junto ao relógio) através da seguinte figura: 

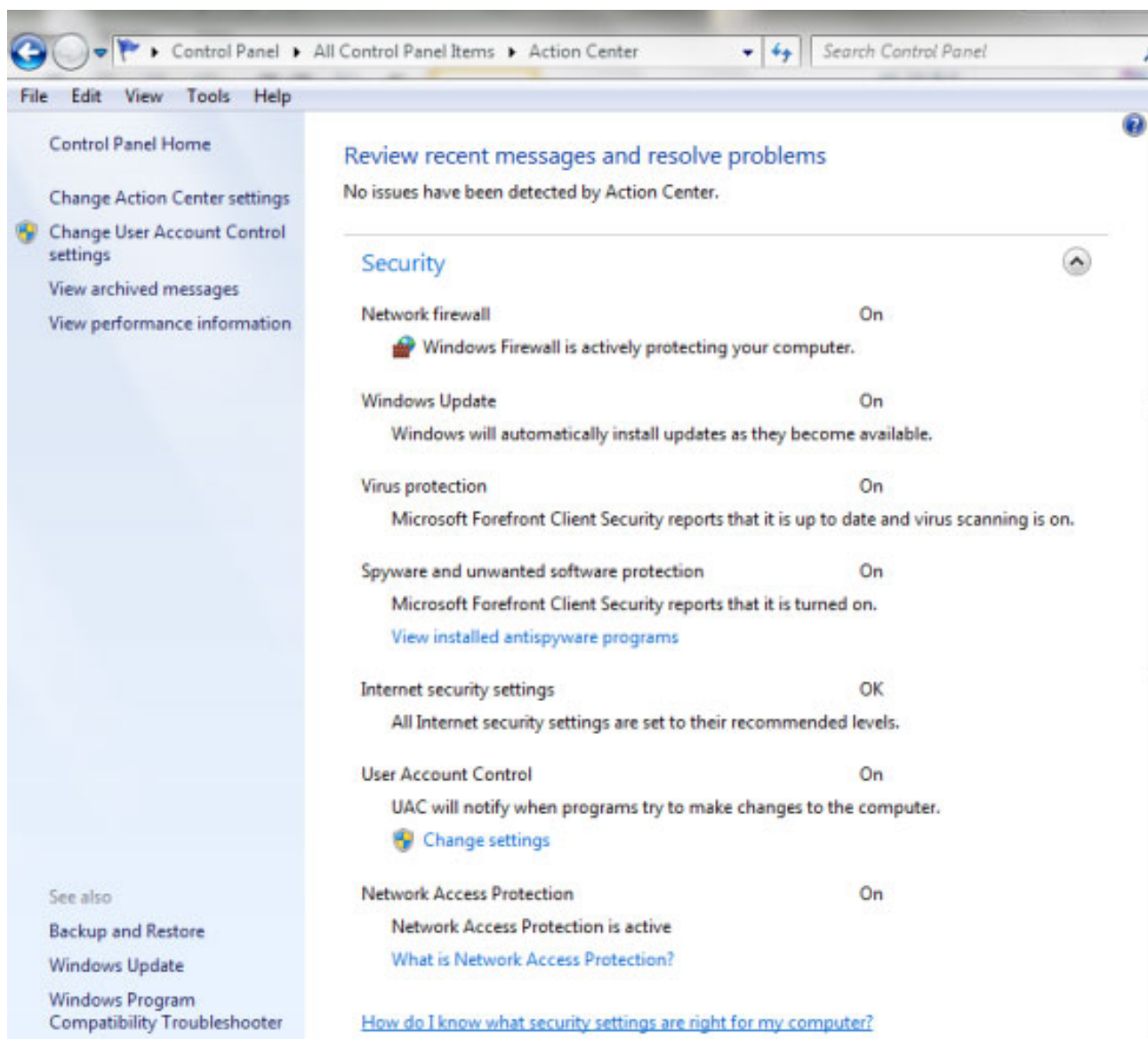


Figura 2: A segurança vista através do *ActionCenter*

ActionCenter: Segurança

Escolhendo a opção relacionada com a segurança, temos acesso a informação sobre as diversas áreas (figura 2), tais como:

Windows Firewall - que deverá estar activa. Nos dias de hoje, com a permanente ligação dos computadores à Internet, é crítica a existência de uma *firewall* no computador. A sua inexistência torna o computador vulnerável a ataques.

Windows Update - deverá estar em modo automático, ou seja, o computador deverá estar programado para descarregar e instalar as actualizações tão rápido quanto possível.

VirusProtection - mais uma peça fundamental na segurança. Qualquer computador deverá ter instalado um antivírus e esse mesmo antivírus deverá estar devidamente actualizado. Um antivírus desactualizado, muitas vezes, é tão ineficiente quando a sua inexistência. É por isso que o *ActionCenter* monitoriza tanto a instalação como a actualização do antivírus.

Spyware - uma boa protecção deverá ter em conta os vírus mas também o *Spyware* que nos últimos anos tem crescido de uma forma exponencial.

Internet SecuritySettings - os parâmetros de segurança são analisados neste local, quando navega na Internet. Deverá aparecer um OK, se não for o caso, não navegue na Internet até estar em perfeitas condições, ou seja, até reportar um OK neste local.

UserAccountControl - deverá estar ligado. É aqui que é monitorizado quando os programas alteram as configurações no computador. Desligar esta opção torna claramente o computador substancialmente mais vulnerável a programas maliciosos.

ActionCenter: Manutenção (cópias de segurança)

Um dos pilares da segurança está directamente relacionado com a disponibilidade da informação na altura que a mesma é necessária. Já alguma vez perdeu aquelas fotos que só existiam em formato digital?

É importante estar preparado para o pior, seja um apagar acidental de um ficheiro ou uma substituição de um ficheiro mais novo por um mais antigo. Pode ser o resultado de um *malware* que simplesmente apaga os ficheiros, ou algo mais desastroso como ficar com o sistema operativo danificado, uma avaria no disco rígido do computador ou a perda / roubo do mesmo.

Quando tiver de lidar com algum dos cenários atrás descritos, é essencial que tenha uma cópia de segurança. Daí ser importante ter em atenção os alertas do *ActionCenter* relacionados com as cópias de segurança.

A segurança para além do ActionCenter: O que fazer para aumentar a segurança dos dados no PC que tem o Windows 7?

Os nossos computadores, especialmente os portáteis, contêm informação confidencial. É normal uma pessoa que utiliza um portátil no trabalho, levá-lo para casa no final do dia ou quando viaja.

E se o portátil for roubado ou se perder? Ter uma cópia de segurança é importante porque nos permite ter acesso à informação. Mas, o que acontece à informação que fica no portátil? Não queremos que esses dados caiam em mãos erradas. Se não forem tomadas medidas especiais, é muito fácil ter acesso indevido à informação de um portátil. Basta tirar o disco rígido e colocá-lo num outro computador para

ter acesso aos dados. Se consegue rever-se neste cenário, então deverá ter em consideração a encriptação dos dados; o Windows Vista e o Windows 7 (ambos na versão Ultimate) já incluem o mecanismo que protege os dados do computador a acessos não autorizados. Todo o disco é encriptado de uma forma completamente transparente para o utilizador. No caso do computador ser roubado ou se perder, o acesso à informação é negado mesmo que o disco seja retirado e colocado num outro computador.

E quando copiamos informação confidencial para uma USB *flash drive*? Quantos de nós é que não perderam já uma *Pen*?

Porque estes cenários são bem mais comuns do que possa parecer, o Windows 7 (versão Ultimate) traz uma grande inovação, a possibilidade de encriptar não apenas os discos rígidos mas também qualquer aparelho removível. E o aparelho externo pode ser utilizado não apenas no computador no qual foi encriptado. Com esta funcionalidade, a segurança atinge um outro patamar.

Fonte: Microsoft

Topo 



Este e-mail é apenas informativo, por favor não responda para este endereço. Para obter esclarecimentos adicionais, sobre este ou qualquer outro assunto, ou efectuar sugestões, e para que o possamos servir melhor e mais eficazmente, sugerimos que visite www.millenniumbcp.pt ou ligue para o número de telefone 707 50 24 24.

Estes e-mails não permitem o acesso directo ao site www.millenniumbcp.pt, não incluem atalhos (links)*, nem são utilizados para lhe solicitar quaisquer elementos identificativos, nomeadamente códigos de acesso. Se receber um e-mail, aparentemente com origem no Millennium bcp, que não esteja de acordo com esta informação, não responda, apague-o e comunique, de imediato, este facto para: informacoes.clientes@millenniumbcp.pt

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço electrónico, aceda a www.millenniumbcp.pt e escolha a opção Contas e, posteriormente, a opção Personalização.

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882

* Alguns serviços de e-mail assumem, automaticamente, links em certas palavras, sem qualquer responsabilidade por parte do Millennium bcp.

www.millenniumbcp.pt

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



Highlights

Trojan Horses

[More +](#)



Basic security principles

Windows 7 Security

[More +](#)

[Versão portuguesa](#)



Highlights Trojan Horses



A bit of background

The expression 'Trojan Horse' first appeared in Greek mythology. The story goes that the Greeks sent the Trojans a peace offering - an enormous wooden horse. However, a group of Greek soldiers were hiding inside it and waited till nightfall to open the city gates and take over Troy.

Modern trojan horses, simply called 'trojans', are bits of malicious computer code which carry out unauthorised actions and may harm, cause unexpected behaviour and put your system's security at risk by opening up a hidden backdoor. This type of computer programme may allow the person running it to:

- **Steal user** credentials (passwords, codes, etc);
- **Steal** personal details stored on your computer;
- **Copy data** (documents, files, etc);
- Create, within your network, **a security breach**, thus granting access to protected areas in the network and allowing others to cause damage.

Trojans often come in the guise of other software and compromise your PC's security. As a result, it affects the confidentiality, integrity and availability of the information stored on the infected machine.

How Trojans get into your PC

Trojans are installed whenever a user carries out a certain action. Possibly by:

- Opening an attachment that came with an alluring email;
- Accessing certain websites, and clicking on certain links that will download and run specific software;
- Installing a CD/DVD someone has offered you containing dangerous software.

Any one of these cases might give way to a trojan entering your system.

How to bring down a trojan

Some protective measures can prevent certain effects malicious code may set off, namely:

1. Using antivirus and antispymware software and keeping it updated, applying its patches and security fixes;
2. Using a firewall;
3. Setting up your internet equipment correctly.

But just technology won't cut it.

All this may not be enough if you end up working against the protection you've put in place, usually at some financial cost. When users:

1. Give their credentials or personal codes to others who use them to their own advantage;
2. Open emails and attachments just out of curiosity, without first confirming where they come from and what they're about;
3. Access certain alluring sites and download certain *software off them*;
4. Install software they don't know the origin of;

no amount of security measures will help you overcome these self-inflicted obstacles.

We can conclude that: **Security starts at home and to a great extent depends on our attitudes.**

Here's an everyday example: you might try to protect your home with the most sophisticated equipment, but if you give access to your house key to someone you don't trust, all your investment will have been in vain. The same principle applies to PCs and the use we make of them.

In conclusion: Trojan Horses are malicious bits of software that can harm your computer. Nonetheless, we can take them out by taking all the necessary steps.

Protect your computer. A lot depends on you!

Read our Newsletters and other Security topics at www.millenniumbcp.pt.

Source: millenniumbcp.pt

Top 



Basic security principles

Windows 7 Security



Windows 7 has brought about a series of new possibilities. This operating system, besides allowing for a more streamlined PC, was designed having security as a primary concern.

Security is, without a shadow of a doubt, a very vast subject. With this text we intend to show users of new technologies, especially home users, what they can expect from Windows 7 security features.

The security hub in Windows 7: ActionCenter

Tired of pop-up windows? ActionCenter helps you decide which Windows 7 alerts should pop up and which should not.

ActionCenter is the heart of the main security events in Windows 7.

As you can see in figure 1, in ActionCenter you can find not only security but also computer maintenance items.

If Windows 7 needs maintenance, you'll see it in ActionCenter.

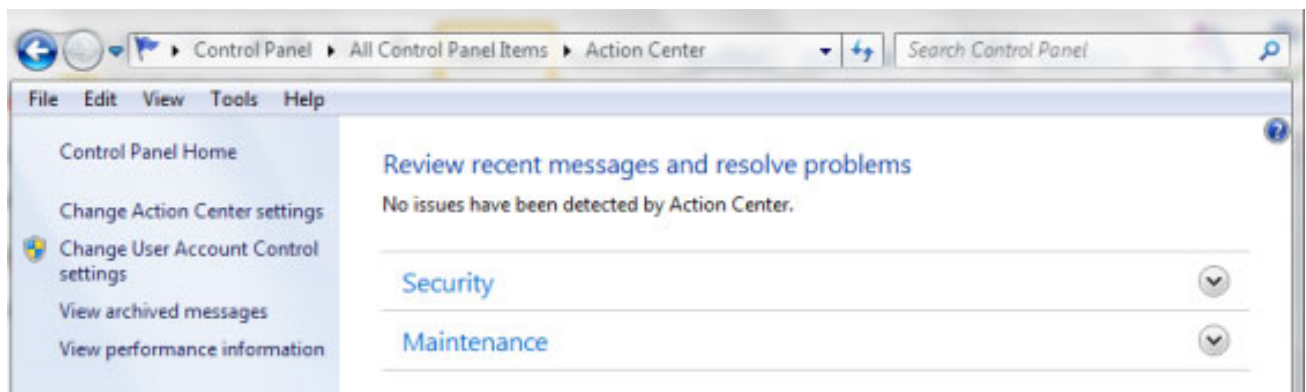



Figure 1: Options in ActionCenter

This is where you can find the notifications and steps to take to help you keep your PC safe and working properly. If there's an item in ActionCenter marked red as Important, then you should try to solve it as soon as possible. For example, your antivirus might not be updated. If the notification is marked in yellow, that means you have maintenance tasks which you need to take into account, as for example, making backup copies.

ActionCenter notifications will appear on the bottom right-hand corner of your screen (next to the clock), with the following icon: 

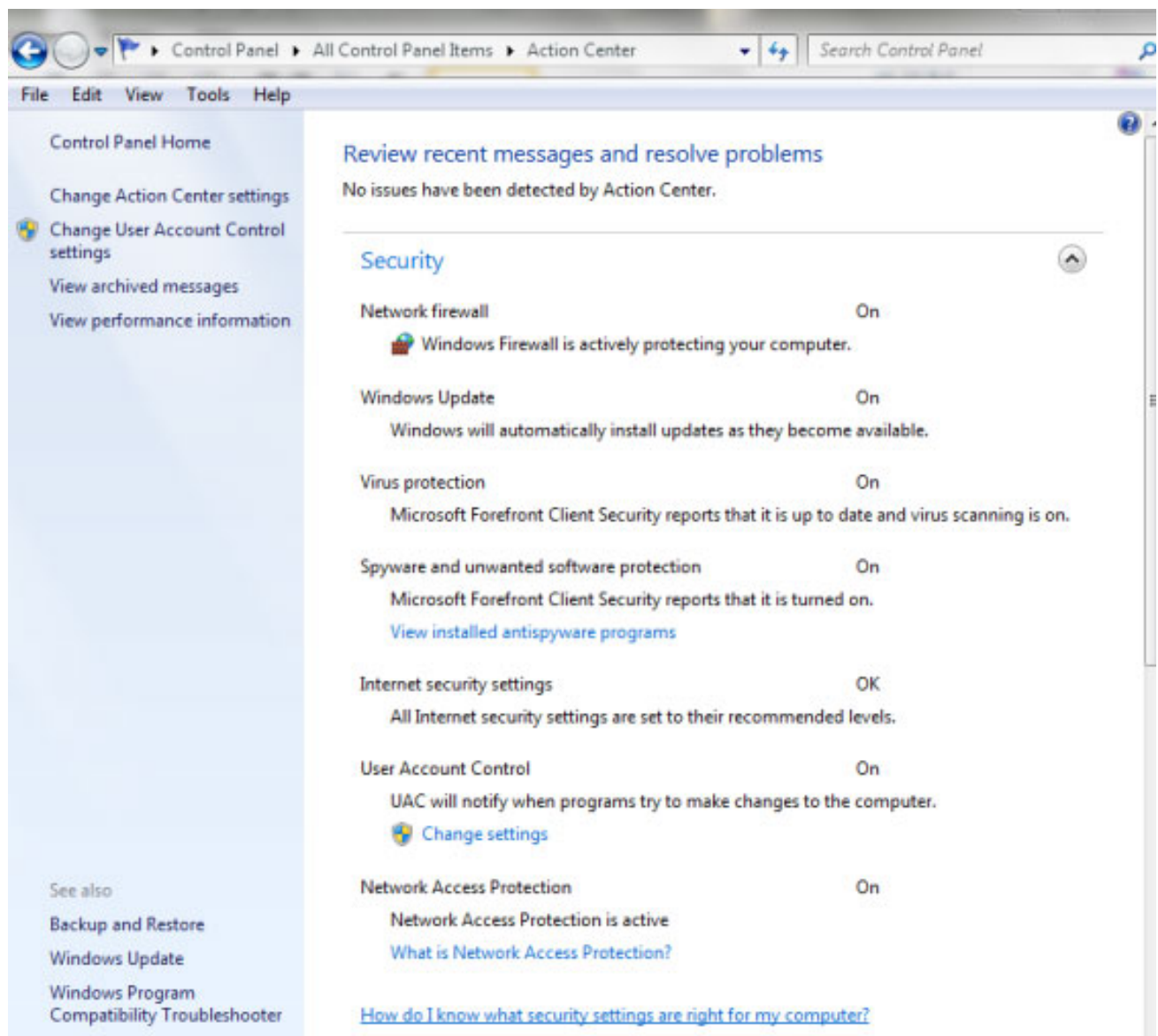


Figure 2: Security view in ActionCenter

ActionCenter: Security

On the Security screen, you can find information on a number of items (figure 2), such as:

Windows Firewall - should be active. Nowadays, with computers permanently connected to the internet, it is critical that your PC has a firewall. Not having one leaves your PC open to attack.

Windows Update - should be on automatic, i.e. your PC should be programmed to download and install updates as soon as possible.

VirusProtection - another essential security item. PCs should always have antivirus software, installed and updated. If your antivirus is not up-to-date, it's practically the same as not having anything! That's why ActionCenter continually monitors whether you've installed antivirus software and are keeping it up-to-date.

Spyware - good protection involves not only viruses but also spyware, which has grown exponentially over the past years.

Internet Security Settings - this is where your security parameters for surfing the internet are. There should be an OK sign next to it. If not, don't surf the internet until it is on.

UserAccountControl - should be on. This is where the system monitors changes made to your PC. Turning this option off will clearly leave your PC more vulnerable to malicious scripts.

ActionCenter: Maintenance (backup copies)

One of the reasons for computer security is directly related with you having your data at hand when you need it. Have you ever lost those photos you only had in digital format?

You should be prepared for the worst - the accidental deleting of a file or the wrong replacement of files. It could be the result of malware that is simply deleting your files, or something more disastrous could happen, like damage to your operating system, causing your hard drive to malfunction or crashing/stealing data from it.

If you are forced to deal with any of these scenarios, it is imperative that you have a backup copy. That's why ActionCenter backup alerts are so important.

Security beyond ActionCenter: What can you do to boost the security of your files in Windows 7?

Computers, especially laptops, contain confidential information. It's normal for people who use their laptops at work to carry it back home at the end of a day's work, or when they travel abroad.

What if you lose your laptop or it gets stolen? Having a backup copy is essential to be able to access your information again. But what happens to the information that stays on your laptop? We don't want it to fall into the wrong hands. If you don't take special measures, it's very easy for others to access the information on a laptop. All they need to do is take out your hard drive and put it into another computer to access the data on it. You should therefore consider encrypting your data; Windows Vista and Windows 7 (both in the Ultimate versions) already include a mechanism to protect computer data from unauthorised access. The whole hard drive is encrypted in a way that is, however, completely transparent to the user. If your computer is lost or stolen, access to the information on your hard drive will be denied, even if the drive is put into another computer.

What if we copy confidential information onto a USB flash drive? Who hasn't lost a pen drive?

Because these scenarios are much more common than one would think, Windows 7 (Ultimate version) comes with a great innovation - the possibility of encrypting not only hard drives but also any portable drive. And you can use these portable drives on other computers as well. With this new function, security has reached a whole new level.

Source: Microsoft

[Top](#) 



This is an automated notification. Please do not reply to this message. We're happy to help you with any questions or concerns you may have and listen to your suggestions. So that we can provide you best service, please go to www.millenniumbcp.pt or dial 707 50 24 24.

These emails do not grant direct access to www.millenniumbcp.pt, nor do they include links, nor are they sent to ask*

for any personal details (namely access codes). If you do receive any such email, apparently sent by Millennium bcp but not in accordance with the above information, do not reply: delete and report it immediately to: informacoes.clientes@millenniumbcp.pt

If you do not wish to receive such information via email or if you wish to change your email address, please go to www.millenniumbcp.pt and click on Accounts, then Customize.

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882

** Some mail services will, automatically, assume certain words as links, without any liability from Millennium bcp.*

www.millenniumbcp.pt

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