Take Steps to Boost the Security of Your Network

The level of security provided by Windows out of the box is fairly basic, meaning that you shouldn't rely on your system to be secure without taking steps yourself to boost the security. Windows has many well-known security gaps that a hacker can exploit with ease. Not only do you face external threats from the Internet, but there is also the possibility of other users on your PC trying to access your sensitive data, meaning that you need to take steps to protect sensitive data by limiting access rights.

Use the following checklist to optimally protect the data on your network:

Task	Description
Check your network structure and firewall configuration	Protect your local network from unauthorised external access with a suitable firewall. You also need to remember that if you connect to the Internet using a router, it will have a built-in firewall that needs to be properly configured.
Configure your router for safe access	Make sure you take advantage of the security features offered by your router, particularly in respect of your wireless network, by enabling 802.1x authentication, WPA2 and MAC filtering, and close all unused ports on the router.
Log in with secure passwords	Creating separate accounts for each user of your PC with their own passwords improves security, since only authorised users have access to important or confidential information. Configuring strong passwords allows you to provide additional protection against unauthorised users.
Check that users have the correct access privileges	Be very careful when assigning permissions to the different users of your PC. Only give a user the security privileges that are necessary for their work. You should also restrict shared folders to certain users or groups.

Task	Description
Regularly backup your data	Daily data backup isn't enough to secure your server. You should also store the backup in another location to your server, so that you can access it following a fire or theft, for example. The latest Trojan threats work by encrypting the data on your hard drive then charging you a ransom to recover your files. The only sure way to combat this is to restore the data on your computer from a backup taken before the infection struck, which is why it is so important to take regular backups, on a daily basis if possible.
Make sure all of your software is up-to-date	Install any software updates and security patches that are available for your system. These will close any gaps in security caused by software bugs, and will also sometimes add additional security features.
Install an anti-virus program	Viruses don't just get into your system via infected emails. They also use services, shared folders on your network, the Internet or even infected files on removable media such as USB sticks. You should therefore have up-to-date anti-virus software installed, and regularly use it to scan your PC for problems.
Data encryption	Encryption programs encode all of your data so that it can be transferred over the Internet in a secure way, and they are a very effective way of ensuring data confidentiality. Firewalls can encrypt the data of an authorised user and allow it to pass through the firewall on to a public network, via a so-called Virtual Private Network (VPN). The firewall that protects the receiving network can then examine the data, decrypt it and make sure that the authenticated recipient gets it.