Information for wireless Users: 10 Steps to a secure connection

i

For your convenience we have summarized the measures to be taken in order to get a secure wireless LAN. Manufacturers of wireless devices sometimes don‘t provide all the necessary information about securing a wireless LAN. Therefore it is understandable that it is sometimes not clear, how you can protect your wireless LAN against intrusion. In the following, we have listed all important points about securing a wireless LAN. With the help of this paper and your product‘s manual, you should be able to get fairly secure. Not all mentioned security measures are supported by every device.
Please don‘t forget: By following this guideline you are not only securing your wireless LAN, but also all your data and applications!

1

Activate WEP encryption (Pay attention: you have to activate it on the access point as well as on all the adapters). Always use at least 128-bit encryption. Don‘t choose a simple string as key but a complex string as e.g. A9FE10. Change the WEP key regularly. This measure gives you better security and protects your systems from unwanted access by third parties.

2

Switch on access control to the access point based on the MAC (Address of a network card). Enter the MACs of the adapters you want to use. This measure protects your network against unauthorized access by third parties.

3

Name your SSID/ESSID in a way, that no correlation between the name of the network and its owner can be made. **The owner of this access point cannot be identified by the name of the network.**

4

Hide your SSID. (NO SSID Broadcasting) **Hiding the SSID makes your network non-public. Be cautious, doing so may also cut you off of your own access point.**

○ Required measure

● Optional Measure

i Information

S Support

§ Legal information

! Important

5

Change your username/password on your access point frequently. Choose a complex password, avoid simple to guess passwords.

6

If you don‘t use your wireless network for a longer period, switch off your access point. This prohibits any intrusion during that time.

7

Don‘t connect your access point to your internal LAN, if you are not sufficiently shielded against attacks from the outside. Protect your network shares with a password, increase your access protection on workstation and servers.

8

Protect your PCs and Servers by a software firewall. **Activate access protection on all systems.**

9

Never write down your passwords, don‘t use them twice. This reduces the probability of an intrusion.

10

Check your log files for possible attacks.

S

You can get support for various problems at the independent discussion platform

www.wireless-forum.ch

W F
Wireless-Forum

§

Beware of unprotected wireless LANs. You can be held vicariously liable.

!

According to a statistic of www.wireless-bern.ch approx. **60%** of the access points **are NOT encrypted.**
Please note: Most of the aforementioned security functions are switched off at the time you buy your wireless product.