Secure your WiFi network

CHOOSE A STRONG PASSWORD

- ✓ Change the default password for your WiFi and the Web interface and choose a strong password. This means you should not use for example your last name, zip code or date of birth.
- ✓ Use the WPA2-AES encryption, because alternatives like WEP are not secure.

CHANGE DEFAULT NAME OF YOUR WIFI NETWORK

The default name of your wireless network mostly consists of the router type of brand. Routers that are susceptible of hackers, stand out this way.

- ✓ Change the name of your network without using traceable names like your last name, address or home number.

TURN OFF SETTINGS

We advise you to turn off the following settings:

- ✓ **Turn off remote access**
  With remote access your router configuration is open for internet and others can easily give themselves access to your router and settings and change them.
- ✓ **Turn off WiFi Protected Setup**
  With WiFi Protected Setup you easily connect devices to each other using WiFi. In many routers, this technique is not secured sufficiently and can therefore easily be breached. When you do need WPS only turn it on temporarily.
- ✓ **Turn off Universal Plug and Play**
  Universal Plug and Play helps you to connect devices without difficult configurations. This technique comes with many security risks, so hackers can easily access your devices via internet.

INSTALL UPDATES

Hackers can target connections on almost any device connected to WiFi if these devices do not receive updates.

- ✓ Make sure all your devices are regularly updated.
- ✓ Check at least once a year whether there is an update available from the manufacturer for your router.
- ✓ When possible turn on automatic updating.

USE A GUEST NETWORK

A guest network is strictly separated from your own network. In this way they cannot access your files and devices (like your printer).

- ✓ Set up a guest network with a unique and strong password for your visitors.
- ✓ The security of smart devices is often insufficient. By connecting them only to your guest network, hackers who use these leaks in security cannot reach your own network as easily.