WLAN

Whether at home, at work or in a public space: Today you can go online just about anywhere and at any time. This often involves the use of a WLAN.

Protect yourself by...

- only making limited use of unknown WLANs or avoiding them altogether, if at all possible.
- not using public WLANs for e-banking and generally never transferring any confidential data this way.
- whenever possible only connecting to encrypted WLANs.
- using a current encryption method (WPA) with a strong password for your own access point.

Operating principle

Using wireless technology, WLANs offer an extremely flexible, convenient way of connecting to a network and the Internet via a mobile device, without the need to worry about annoying cables. For mobile devices, such as tablets, it is often the only way to connect to the network anyway. This type of connection is also frequently activated on smartphones.

However, using and operating such wireless networks also has some inherent risks which many people are not even aware of.

Using WLAN securely

Apply a “healthy” dose of suspicion when using an unknown WLAN.

If at all possible, connect only to encrypted WLANs (WPA2 or WPA3).

Don’t use public wireless networks for e-banking, and don’t transfer any confidential data across them, for instance via “hotspots” in public spaces (towns, stations, etc.) or hotels.

Use end-to-end encryption for any confidential data, no matter which type of transmission technology you choose.

If possible, deactivate the “connect automatically” function for unknown and unprotected WLANs on your mobile devices.

Operating WLAN securely

Activate a strong type of encryption, at least WPA, or even better WPA2 or WPA3, and make sure you use a strong network key and password.

Change the network SSID if it contains the name of a person, such as a family name, or any information on the router, e.g. its type.

Replace the factory-set router passwords with your own, strong ones.

Copyright © 2020 – All rights reserved. Lucerne School of Information Technologies

Activate the MAC filter.

If possible, reduce the transmission power of your WLAN router and switch it off if you don't need your local wireless network.

You should also take appropriate precautions if you are running your own hot spots on your mobile phone, to prevent any abuse of your mobile Internet connection.

WLAN stands for Wireless Local Area Network. This method of communicating wirelessly is extremely flexible, convenient and therefore widely in use today.

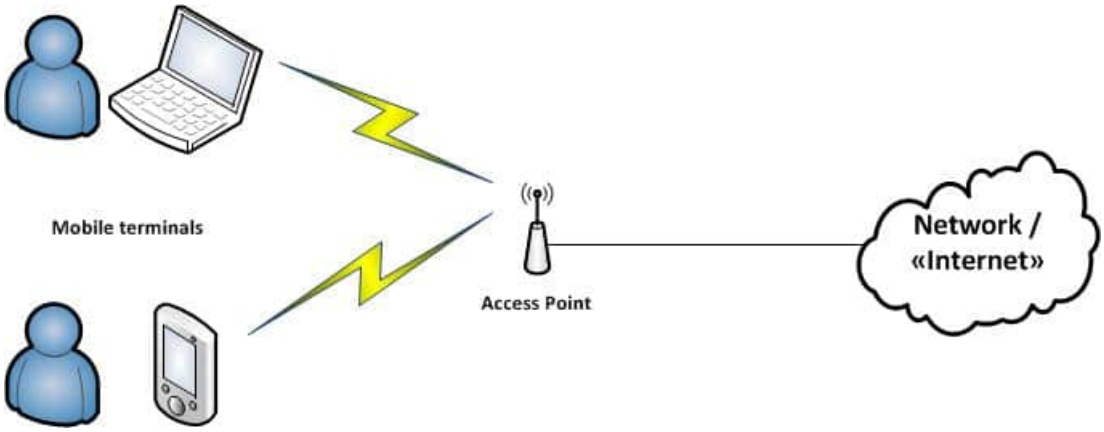
However, using and operating WLANs also has some inherent risks. You can make them considerably more secure with a few suitable measures.

Copyright © 2020 – All rights reserved. Lucerne School of Information Technologies

Further information for those interested

WLAN structure

The central component of a WLAN is the access point. It is the link between the air interface and the mobile devices on the one hand and the cable-connected network and the Internet on the other. The access point "generates" the WLAN by sending out radio signals into all directions via its aerials.



So that devices can "see" the WLAN, the access point usually transmits a network ID - the so-called SSID (Service Set Identifier). Users can differentiate between all WLANs available in a location and select their required connection.

Encryption

The use of wireless transmission has the drawback that it is relatively easy to read out any data transmitted. Generally any device inside the transmission range of a WLAN catches all the data traffic. For this reason, the connection between mobile devices and access point should be encrypted. And although you cannot prevent communications being read out, nobody can then do anything much with them.

There are different methods of encryption:

- **WEP**
  Wired Equivalent Privacy was the first encryption protocol used as standard in WLANs. Meanwhile, this is also considered insecure and is relatively easy to hack. You should therefore no longer use this type.
- **WPA**
  WiFi Protected Access is an advanced form of the WEP protocol. Improved security mechanisms ensure better protection. For instance, network participant authentification was improved, and dynamic keys for transmission were introduced.
- **WPA2**
  WPA2 is built on WPA, but uses the strong AES algorithm for encrypting data transmitted.
- **WPA3**
  WPA is currently the latest encryption standard for wireless networks. In particular, attacks on encryption passwords are made considerably more difficult when compared to WPA2.

Whenever possible, you should now only ever use WPA2, or where available, WPA3 in WLANs. You must choose a sufficiently strong Preshared Key, i.e. the password to the network. It should at least be 16 characters long and have all the characteristics of a strong password (https://www.ebas.ch/en/4-protecting-online-access/) .

Copyright © 2020 – All rights reserved. Lucerne School of Information Technologies

In this regard, you should also note that this only protects the distance between the terminal and the access point. This encryption ends at the access point, so that from here on onwards, data will once again be transmitted in an unprotected manner. Regardless of the transmission technology, confidential contents should always be encrypted end-to-end by the chosen transmission technology, e. g. when surfing the Internet or when e-banking, with a TLS/SSL encryption (https, lock symbol).

MAC filter

Every network device has a MAC address, i.e. all mobile terminals too. This always acts as a unique identifier. Access points offer the option of using a MAC filter. This means only registered mobile devices with a known MAC address are permitted to access the network.

However, a device MAC address is not tamper-proof. With the right tools, an authorised MAC address can be faked, thus circumventing this filter. However, the MAC filter option should still be used, even if it just serves to erect another barrier against potential attackers.

Copyright © 2020 – All rights reserved. Lucerne School of Information Technologies