Suomen Suunnistusliitto

Data security guidelines for orienteering competitions

Introduction

When considering data security in the context of an orienteering competition, the key elements are the digital map and course information. Current technology exposes a map used in digital form for many risks, of which the most critical ones are:

- Users' lack of knowledge about risks
- Users' carelessness and accidents in using the digital material
- Attacks aimed at systems, and social hacking

In the IT world, in the context of data security, the discussion is often about reducing the so called 'attack surface', which aims to make it as difficult as possible to attack the system. This approach can be applied to digital map and course material too. By minimising the number of people dealing with the map and the time when the data is available, the risks for data leaks and accidents are minimised in the most effective way.

When it comes to data security, the weakest link is the user himself, and not so much the systems that are used to handle the material.

This document goes through the key issues regarding the data security of an orienteering competition, but the document is not exhaustive. The document is meant in the first place for the course setter, course controller and event adviser of an orienteering competition. The more important the competition is, the more carefully these guidelines need to be followed.

These guidelines apply to matters related to data security. The document does not directly address attempts to defraud or to break the sport's rules; it is created to prevent problems with data security of orienteering competitions.

Information security guide

The concerned party (course setter, course controller, event adviser) must ensure that:

1. System passwords are strong and are changed often enough. A good password is first and foremost long (at least 12 characters) and contains special characters as well as upper- and lower-case characters. It is recommended that your email and data sharing service passwords are changed when you start planning a new competition. Generally, the passwords should be changed at least every 6 months.

2. System identification should whenever possible be strong identification, by using two different authentication methods.

3. Security settings of the data sharing services used should be checked and set to be as restrictive as possible. Special attention needs to be given to services with public security settings as default.

    - Data sharing services online can be a problem if
        - Security settings are weak, and sharing is public
        - There is automatic synchronization between devices
        - The passwords are weak

4. Photos taken of the map shall not be sent in digital form via email. Photos of the map should not be taken with a mobile phone. This decreases the risk for various possible data leaks via social media or cloud services.

    - Taking/sending photos of the map using a mobile phone can be a problem for example if
        - The files are automatically synchronized into a cloud.
        - The recipient group in a messaging app is unnecessarily large
        - The message is sent to a wrong address or group
        - Devices are updated to a new version

5. Map files sent via email are encrypted whenever possible.

    - A map as an email attachment can be a problem for example if
        - Unencrypted map files are used
        - Weak passwords are used
        - The map is attached as a picture and automatically saved into a cloud

6. The system passwords are always sent via SMS or phone. Email or private messages on social media may not be used to send passwords.

7. The number of people dealing with the map and the time they have access to the map is limited. Paper maps shall always be collected back. A record should be kept of the people who handle the map and course files.

When dealing with map and course files, it is important to remember that the following actions may also create a data security risk:

- Handling information about TV schedules, camera locations, and similar
- Handling information related to GPS tracking
- Sharing competition information with the media beforehand
  - Information must not be shared with people who don't need it
  - In any case, the time window for the necessary material to be shared before the competition should be as short as possible

8. It is ensured that all people dealing with the map understand the sensitiveness of the data. Especially when organising a major event, there may be stakeholders involved who do not have knowledge of the sport and therefore do not have the necessary understanding of the topic.

9. GPS watches are used as little as possible in test runs. The safest way to protect against data loss here is to completely forbid the use of GPS watches that record the tracking. It should also be forbidden to carry a mobile phone on a test run.

   GPS watches or smartphones can be a data security problem if
   - The GPS routes leak online from the watch
   - Any pictures, or other information about the terrain, are shared on social media

10. The possibility for data system infiltration is kept in mind, and the systems appropriately configured and updated. It is important to be always prepared for so-called social hacking, or other kind of 'fishing' attempts for sensitive information.