Punainen Risti

Updated: 8 September 2025

BRANCH GUIDELINES

Data security guidelines for volunteers

General guidelines

- Keep personal data away from the eyes, hands and ears of outsiders.
- Do not discuss confidential matters in public.
- Use a passcode on your mobile device and a privacy filter on your laptop screen.
- Lock your laptop when leaving your workstation (Windows + L).
- Do not leave your devices unattended.
- Avoid open and unsecured networks. Only use known and password-protected networks.
- Use strong passwords and multi-factor authentication for your accounts.
- Choose your apps carefully and keep them updated.
- Reboot your devices weekly.
- Treat strange emails and phone calls with healthy suspicion.

Strong password

A good password is long (at least 15 characters) and contains both upper and lower case letters, numbers and special characters. Use a unique password for each service. Never tell anyone your password.

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) means that, when logging in, you must confirm your login with a second form of authentication, such as a confirmation code sent to your phone. MFA significantly improves security because even if your password is leaked or falls into the wrong hands, an attacker cannot log in without the authentication method in your possession.

Therefore, enable MFA whenever possible.

Only accept MFA requests when you are attempting to log in to the service yourself. If you receive a sudden or unexpected confirmation request on your phone, do not accept it, as it may be a sign that someone is trying to access your account without authorisation.

Suspicious messages

If you are unsure about the sender or content of a message you have received, verify the matter by calling the sender, for example.

If you receive a suspicious message, do not open any attachments or links in the message. IF you accidentally click on a link in a message and it takes you to a login page, do not enter your username and password.

If you have clicked on a suspicious link or entered your credentials on a suspicious website, change your password **immediately** and contact FRC IT support at itspr@redcross.fi.

Signs that you can use to identify a scam message:

1. Suspicious sender address
   At first glance, the address may appear to be genuine, but it differs slightly from the real address (e.g. m1crosoft.com vs. microsoft.com).
   Hover your mouse over the sender's address to see the actual sender. Do not rely solely on the sender's name; also check the sender's email address.

2. Beware of urgent and threatening messages
   Scam messages try to create a sense of urgency: 'Your account will be closed', 'Act now', 'Payment required immediately'. Scammers may also engage in blackmail and threats by threatening to damage your reputation or cause you to lose your assets, for example. The goal of these messages is to prompt you to act quickly without thinking.
   Take your time and think about whether the message sounds logical and whether you would expect to receive such a message.

3. Grammar and spelling mistakes
   Read the message carefully. Scam messages often contain numerous misspellings, poor grammar and translation errors. Incorrect grammar can be a sign of an AI-generated scam message.

Also check the layout and signature of the message. Is the message missing a logo, contact details or perhaps an official signature? Authentic messages usually feature recognisable branding.

4. Check any links before clicking
   The text in the link may appear genuine, but in reality, the address may take you to a scam site. Check the authenticity of the link by hovering your mouse over it and see where it actually takes you. If you are not sure about the authenticity of a link, do not click on it.

5. Never give out your password or personal information
   Trustworthy parties will never ask for your password, bank details or personal identifiers by email. Only enter your credentials on official login pages and use multi-factor authentication whenever possible.