Compromised account procedure

All rebels with an account on the UK Hub, UK Forum, Global Mattermost and UK Cloud – which gives them access to material that should not fall into unfriendly hands, or that may compromise the legal position of themselves or others, for example, through providing evidence for conspiracy charges – **need to be aware of these procedures.**

Precautions to take when access to an account Is compromised

The steps below allow for the rapid temporary suspension of a compromised account on all XRUK services, to be followed either by reinstatement of the accounts with fresh passwords, or permanent deletion of the account as appropriate.

1. Set up, on the UK Hub, a **secret codeword** or phrase which you can easily remember and speak without having to spell it out, and that does not have ambiguous spelling.

   - Log in on the UK Hub and click on the 'Set My Codeword' icon.

   - Enter your phrase or word in the box.
   - Once set, you can find and change your codeword by clicking on the Admin button and navigating to 'My Settings'.

2. Follow the advice available through the links below to **secure any device** that you use to access XR services and email (these were written for a previous Rebellion but are still relevant):

   Laptop Security Guide

   Phone Security Guide

   This should include any desktop devices you may leave at home that could be subject to a search warrant and seizure in your absence.
   There is not yet a specific general guide to securing desktop devices against seizure – much of the laptop advice applies. Don't forget any memory sticks or CD/disc backups you may have lying around.

3. **DO NOT** take any device, which has general access to your Hub accounts, into an arrestable situation! Please use a **'burner' phone** and only install and use **secure apps** on it. See the Phone Security Guide above.

4. If you have operational reasons for needing access to XR online services (other than Signal and Telegram and areas like the public website that do not require a login and can be viewed by anyone), you must be especially careful to ensure that your device is secure and that you don't lose it.

Loss of Your Device – Arrest, Loss or Confiscation

1. If you are arrested, tell your secret codeword to Back Office (Arrestee Watch) or a friend, ideally before your arrest, or if you are arrested without warning, as soon as possible afterwards (e.g. use one of your custody calls to tell Back Office).
2. If you lose your device, or if it is confiscated by the authorities, immediately let your Group Admin or Interal/External Coordinator know, so that they can inform the Hub Admin team.
3. The Back Office Volunteer, your Group Admin or Hub Admin on being told your secret phrase and that you have been arrested, or had a device(s) confiscated, will cross-check the secret codeword and if it is valid, immediately lock all of your accounts – the Hub, Forum, Mattermost and Cloud – until you are cleared. For Group Admins, here is how to deactivate and reactivate someone.

Restoring Your Hub Accounts

1. When you are released, your accounts can be restored. You will need to contact your Group's Coordinator(s) and/or Group Admin for them to restore your account.
2. If any of your devices are lost or remain with the authorities, you will need to **change the email address you use for the Hub**. This change must be done before your account is restored and it is recommended that you change your email even if your devices have been returned. Your new email address should be given to the Hub Admin via your Hub Group Coordinator/Group Admin. A new **Hub Password** will also be issued, and you should subsequently change this. Once the new email has been registered and the Hub account restored, you will be able to access all of your Hub Group information as before.
3. If you are a member of Mattermost channels that the Hub does not know about, your membership of those channels will not be restored automatically. You will need to rejoin these by asking people in them to invite you again.

Non-Hub Services

1. The above ONLY applies to your **Hub, UK Forum, Mattermost, UK Cloud and Vault** accounts. If you have administrator or moderator access to any service that gives you visibility of others' account details or activity, then it is **essential** that you follow a similar procedure for those services as well.

2. For **social media accounts**, it is worth having a trusted close friend/partner who knows your password and can be instructed to change the password immediately should they hear you have been arrested.