Internews Recommendations on Security

Provided by Chris Walker (and later extended by Robbie Mackay), providing advice on using Ushahidi in a place like Syria:

- Create and use limited-privilege moderator accounts
- Admins should install NoScript for Firefox or NotScripts for Chrome
- Admin's should remain logged out as much as possible
    - Only login when you are actively reviewing reports
    - Avoid doing other tasks while reviewing reports
    - This reduces risk of various hijacking attacks
    - Always log out when you're done. Don't leave your computer logged in and unattended
- Do not rely on the "Trusted report" feature
- Require HTTPS
    - Train admins to check the URL and make sure the SSL certificate is valid
- Enforce good passwords
    - How to create secure passwords
- Train moderators to recognize (and delete) suspicious URLs in reports
- Train moderators carefully
- Delete all reports that you do not intend to use
- Have people manually scan submissions to remove personally identifiable information
- Acknowledge and clearly explain that all SMS input is completely visible to a telco or government-level adversary
- Do not allow the map to update in realtime (so as to avoid clearly and immediately identifying victims to perpetrators)
- Disallowing public, Web-based write access entirely? Password-protecting even the read-only map? (Depending on your target audience, of course....)
- It's worth reiterating that you can't have a "do no harm" philosophy without being genuinely open to the possibility of doing nothing...if you judge the risks to be serious enough