DARKDATA
project

Security Essentials for Humanitarian Organizations

1. Collect as little data as possible. Do not collect data proactively. Anonymize and/or aggregate whatever data you do collect, to whatever extent you can.
2. Adhere to the principle of least access. Granularly restrict data to those with a need to know. Depermission frequently, and delete upon request.
3. Use and enforce strong, unique, perishable passwords which are stored in an industry-grade password manager. Never provide "password hints." Augment with MFA.
4. Use secure communications wherever possible. Email and SMS are not secure communications protocols. Be alert to phishing.
5. Don't share accounts, logins or passwords.
6. Lock down your hardware. Promptly implement updates, patches and firmware customizations. Adopt a "thin client" posture.
7. Be aware of, and conform to, security and privacy legislation in all jurisdictions where you operate. Plan for disaster.
8. If you believe your organization has been specifically targeted, have a security professional perform an urgent risk assessment.