New America

OPEN TECHNOLOGY INSTITUTE

Create a Digital Safety Plan

Secure Communications

- [ ] Use privacy-protected, encrypted services to protect sensitive communications (text, voice, video, email, file, cloud storage, etc.)
- [ ] Move conversations with trusted contacts off social media channels
- [ ] Limit access to sensitive files and databases and require passwords
- [ ] Enable waiting rooms, passwords, or locked meeting for video calls
- [ ] Activate disappearing messages or set expiration dates on messages and co-working documents

Safe Web Practices

- [ ] Use privacy-focused browsers or Virtual Private Networks (VPNs) and avoid connecting to public WiFi
- [ ] Confirm website and transaction security by looking for the lock symbol next to the url
- [ ] Don't click or open links, attachments, or QR codes from unknown senders
- [ ] Report, block, flag suspicious activity
- [ ] Offer staff phishing training
- [ ] Turn off or delete browsing history
- [ ] Reject unnecessary cookies and adjust settings to limit third-party tracking and targeted-ads

Account Security

- [ ] Use a password manager to generate and manage complex passwords across accounts
- [ ] Update passwords regularly
- [ ] Activate two- or multi-factor authentication (2FA/MFA) for critical accounts
- [ ] Audit access to shared accounts, files, databases, etc.
- [ ] Activate security alerts for account changes
- [ ] Use a hardware token to access accounts

Protect Devices

- [ ] Password protect devices
- [ ] Regularly update device software
- [ ] Use separate work and personal devices
- [ ] Limit unnecessary app permissions
- [ ] Delete unused apps
- [ ] Turn off ad-identifiers on devices

Social Media Management

- [ ] Set up organization specific accounts and limit login access
- [ ] Adjust settings to hide personal information, account activity, and followers
- [ ] Edit who can interact with your account and report trolling accounts
- [ ] Avoid sharing frequented locations directly or indirectly
- [ ] Get consent before sharing photos about staff, volunteers, or community members
- [ ] Report and block hateful and trolling accounts
- [ ] Audit past posts to ensure information limits
- [ ] Use a data removal service to help remove personal information available online about you

Organizational Data Practices

- [ ] Collect only the data needed to meet organization aims
- [ ] Make data collection and use opt-in and get clear and active consent
- [ ] Store sensitive data in password-protected and encrypted files
- [ ] Delete all data that is no longer needed
- [ ] When possible, dedicate budget and staff to tech support and safety