

Own Your OSINT – Privacy Actions Checklist

As mentioned multiple times, privacy and security are long-term matters. You won't reach a point of satisfaction immediately; once you do, you're very likely to become dissatisfied if you keep up with your privacy.

However, the provided checklists are designed to give a kickstart to your personal security and privacy. These checklists are not comprehensive and couldn't possibly be ... your threat model will be different than mine and you will find additional things "to do". With that, here are the checklists.

Security Checklist

- Full disk encryption on devices
- Breach check on your current data
- No biometrics as primary sign in... replace with pins and passwords
- Biometrics on as an extra layer ON TOP OF passwords/pins
- Password manager
- 2FA on everything (hardware key or 2FA app, SMS if you must)
- Separate "critical" vs "other" apps into different 2FA methods
- Don't carry private information on you
- Store private information in self-hosted or trusted cloud, not on devices
- Audit all your digital services, get rid of any you don't need (including mobile apps)
- Unique usernames and passwords for everything – random generation
- Email "tracker" tags
- "Burner" credit cards to mask banking and personal information
- PO Box / CMRA
- Linux OS or locked down Windows
- GrapheneOS for mobile
- Use private messaging like Signal instead of SMS
- Secure home network

Use the following space to add any additional security items you may want to tackle:

Privacy Checklist

- Disable location services
- Remove EXIF data from photos
- Delete social media (at least make it anonymous)
- Use a VPN
- Privacy-oriented web browser
- Privacy oriented search-engine
- Obfuscate your data online
- Don't give out legal information unless legally required to
- Register domains for email / personal use (use a provider that anonymizes your registration)
- New, anonymous "root" email (never give out)
- New email for personal use only
- New email (professional, behind domain) ... anonymous
- New email (professional, behind domain) ... real name
- A variety of anonymous emails to use for other online services
- New phone number to point VOIP numbers to
- New phone number (VOIP) for personal use only (or reuse existing)
- New phone number (VOIP) for employer
- New phone number (VOIP) for shopping
- New phone number (VOIP) for other online services
- Public Alias
- Regular OSINT-probes to find weak points in security/privacy
- Consider self-hosting as many cloud-based services as possible
- Data broker opt-outs

Use the following space to add any additional privacy items you may want to tackle: