**The 10 Rules of OPSEC**

**Grugq.github.io**

* **Hacker OPSEC blog with guidelines**

1. **Keep your mouth shut**
   * + Never revealing operational details
     + Don’t tell people that you use a nest of VPNs or Tor etc.
     + E.g., messaging a fellow freedom fighter that Tor is slow will reveal operational details
     + Don’t reveal plans of what you intend to do
     + Don’t talk explicitly in public places, use codewords etc.
2. **Trust no one**
   * + Assume everything and everyone cannot be trusted
     + Mitigate the risk through distributing trust
     + Info only to be given out on a necessary basis
     + Definitely don’t trust co-conspirators, can become criminal co-defendants if they are arrested
     + People won’t go to prison for you
     + Watch people who offer to buy information
     + Operate alone
     + Be careful of co-conspirators that disappear and reappear, could now be under control of adversaries
3. **Never contaminate identities**
   * + Don’t share anything between aliases, ip, OS, passwords, emails, friends, cookies, browsers, locations
     + Don’t use different aliases at the same time
     + Don’t visit sites and locations associated with aliases with your real ID
       - i.e., don’t log in to your real fb account whilst on Tor as a different alias, this can be correlated
     + Never log into accounts as an anonymous alias through Tor, that you have previously logged into without anonymising
       - Can associate anonymous connection with real IP
     + If you’re using offsite networks like internet cafes for anonymous aliases, don’t take your phone as this can be linked
     + Don’t use an internet connection from your home to use an alias
       - Otherwise always use an anonymising service if so
     + Always use aliases in separate security domains
     + One phone for one identity
       - Don’t call contacts from on ID with a phone from another
4. **Be uninteresting**
   * + Fly under the radar
     + Avoid high risk areas and actions
     + Don’t hang around on hacker forums if you’re a hacker freedom fighter
     + Don’t maintain accounts
     + Don’t draw the attention of a well-versed adversary
     + Don’t perform actions that could shine a light on you for further investigation
     + Establish an average, believable identity
     + Don’t do anything longer than you have to
5. **Be paranoid now, instead of when you get caught**
   * + Consider all angles form your adversary’s perspective
       - They will always look for easiest ways to catch you so tighten up the simple things first
     + Be aware at all times
     + Plan for things going wrong and mitigations
     + Plan for a knock at the door
     + Use fail-safes or fail-close technology
       - VPN kill switches
       - If something fails, it must fail in a way that continues to protect you
     + Disable Bluetooth webcams and microphones, mouse, keyboards, monitor
     + Switch off other devices when talking about sensitive info
     + When using someone else’s Wi-Fi, use all the same security parameters you would at home
       - Ip could be linked to physical location and time which could be enough to ID you
     + Never leave your devices unattended
       - Power off devices especially when using whole disk encryption
     + Never discuss security, privacy or anonymity matters in public
6. **Know your limitations**
   * + Operate at the level of your abilities
       - If you don’t fully understand what you are doing, then either stop what you are doing until you do, or accept the risk that your lack of knowledge could get you caught
     + Keep things simple, when things get too complex, it could go wrong
7. **Minimise information**
   * + No information = no crime
     + Avoid logging anything, keep operational that you need, destroy everything else
       - E.g., browser history is not required
       - Better to delete it than to encrypt it and keep it
       - Minimise what people can find, even if its fully protected
     + Send as little info as possible in communications
       - ‘I’ll bring the thing’, ‘tell the guy’
     + Don’t send cleartext messages, everything should be encrypted
       - Even non-sensitive info should be encrypted because if not, then encryption alone can give away that the information is sensitive
     + Never leave anything behind that can be traced back to you
8. **Be professional**
   * + If your adversaries are professional, then you must be professional about it too
       - Don’t be an amateur and get caught
       - Treat your OPSEC, Security and Anonymity with the seriousness it requires
     + Take a logical and systematic approach to what you are doing
       - Treat it as a business, don’t make it a pursuit of pleasure
9. **Employ Anti-Profiling**
   * + Avoid revealing personal information used for profiling
       - Even if you believe the messages are private, they are not
     + Never reveal real gender, location, jobs, hobbies, hair colour, height, weight, the cars you like etc.
     + Don’t reveal anything that can reveal your location or time zone
       - Talking about location refs, political events, entertainment events, weather or even using special characters on a keyboard related to your language
     + Avoid keeping regular hours as this can reveal a geographical location or time zone if you do
     + Don’t keep regular routines, habits or methods
     + Use misinformation and misleading info
       - Change your time zone
       - Speak in a different language
       - Use alternative spellings e.g., if you’re from the UK, use US spellings
       - Add metadata to photos and documents, subtly pointing to your fake identity to provide misinformation
     + If our adversaries ask you any questions, answer as your alias and use authorship recognition evasion methods
10. **Protect your assets**
    * + Don’t send data without encryption
      + Choose the right tech and configure it correctly
      + Protect what matters most
      + You’ll know if it worked if you don’t get a knock at the door :)