What can (normal) users do to you protect your privacy online? Consider private browsing mode, VPNs, Tor, anti-tracking add-ons? What are relevant use cases and what risks are involved in the various approaches?

To protect ones privacy, users have a multitude of methods available which complement each other to achieve the common goal.

Aggarwal et. al. state that every modern browser ships with a private browsing mode [1]. In private browsing mode visited pages, cookies, searches and temporary files are not saved to the local disk, while bookmarks and downloads still are. This helps users to protect their privacy from a local attack vector. However, it is important to note that it only protects if the attacker only has access to the pc after the user exits private browsing. Otherwise the local machine could already be compromised by the attacker, f.e. by using a keylogger.

Another feature that modern browsers provide, either direct or indirect through add-ons, is anti-tracking protection. By web tracking it is possible to track a single user over multiple websites, allowing to create profiles or store interests of the user. Very often these trackers are found in advertisements. Bievola et. al. [2] list several extensions that help minimizing the risk of getting tracked, though the first step should be to disable third party cookies, since the third party can identify users by the cookie id. This, however, can lead to inconvenience while browsing. If you don't want to disable all third party cookies at least one of these extensions should be installed: Adblock Plus, uBlock origin, Disconnect, Ghostery or Privacy Badger. These all use different methods to try to find trackers hidden in cookies and block them. Tough even when blocking all third party cookies, users could still get identified and tracked by their ip addresses.

To help preventing that, virtual private networks (VPN) can be used. A VPN is able to tunnel your traffic over a server, only letting the target see the VPN servers ip address [5]. Configuring your own VPN server can be a tedious task and when choosing a VPN service provider you have no control over the VPN server, i.e. the provider is able to log everything you do on the Internet. On the other hand, the same holds for your Internet service provider (ISP), if you are not using a VPN.

To circumvent this single point of trust the Tor Project started in 2002 [3]. Tor is an acronym for "The onion router". The idea is that whenever you target a website, your message will get encrypted and forwarded over multiple relays [4]. Since each relay only knows its predecessor and its successor, the network itself is not able to identify you. However, the traffic from an exit node to your target server has to be unencrypted in order to be understood by the server, i.e. whenever you login or provide personal information of yourself that you also used when not browsing via the Tor network, it is possible to match your browsing

identities. Therefore it is discouraged to use login services, when using the Tor network.

References

1. Aggarwal, G., Bursztein, E., Jackson, C., Boneh, D.: An analysis of private browsing modes in modern browsers. In: Proceedings of the 19th USENIX Conference on Security. pp. 6–6. USENIX Security'10, USENIX Association, Berkeley, CA, USA (2010), http://dl.acm.org/citation.cfm?id=1929820.1929828
2. Bielova, N.: Web tracking technologies and protection mechanisms. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 2607–2609. CCS '17, ACM, New York, NY, USA (2017), http://doi.acm.org/10.1145/3133956.3136067
3. https://www.torproject.org/
4. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. In: Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13. pp. 21–21. SSYM'04, USENIX Association, Berkeley, CA, USA (2004), http://dl.acm.org/citation.cfm?id=1251375.1251396
5. Feilner, M.: OpenVPN: Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using This Powerful Open Source Application. Packt Publishing (2006)