



10 Tips to Safeguard Your Online Privacy

Your digital identity, or *binary tattoo*, is the **permanent** collection of data about you that is available online. Each time you post a picture, status, comment, or click a link, you are adding to that digital identity.

- List the networks for which you have accounts. Remove networks you do not use. Limit the data you submit to only what is needed
- Ensure that your passwords are not language (eg. “Dumbledore”) and have a combination of letters and numbers (eg. “DmblDr54!”)
- Set up multifactor authentication on critical accounts → email, social networks, banking
- Check for apps that you have given social sign-in permissions. Remove any you don’t need
- Change default passwords on IoT (Internet of Things) devices such as WiFi connected appliances, toys, and health monitoring systems (ex FitBit)
- Learn about and be wary of scams. Check return addresses, do not respond.
- Do not plug in foreign USB keys
- Limit use of work email addresses to professional sites and services
- Verify all of your privacy settings. Set a reminder to do this annually
- Turn off your microphone, camera, and geo-tagging in apps where are they not required
- Review your digital photos and remove any you wouldn’t want republished publicly
- Search for and discover your public online identity. Set a Google Alert on your name.

Questions? Comments? We’d love to hear from you: info@binarytattoo.com

