

Internet Anonymity

- QCLUG

1010010100110101010101101100010110101111010101001010001010101001001010101001010100101000110010101001

1010010100110101010101101100010110101111010101001010001010101001001010101001010100101000110010101001

11010010

1010010100110101010101101100010110101111010101001010001010101001001010101001010100101000110010101001

1010010100110101010101101100010110101111010101001010001010101001001010101001010100101000110010101001

1010010100110101010101101100010110101111010101001010001010101001001010101001010100101000110010101001

Introduction

Definition of Anonymity:

- Derived from the Greek word *anonymia*, meaning "without a name" or "namelessness".
- Anonymity means that the real author of a message is not known.

Internet Anonymity

Internet anonymity pertains to users' interaction on the Internet that protects their identities from being shared with another user.

Anonymity is often used to protect the privacy of individuals.

It requires an individual to deal with [an]other entity that does not need any personal identification profile.

Even at the time of dealing, the entity should not identify the individual at all.

The users remain anonymous in their accounts. Anonymity lacks individuality in it. It can be termed as being without a name or with an unknown name.

To gain greater protection of anonymity, some online users utilize several methods to make identification more difficult such as using VPN and Tor.

Source - <http://internet-anonymity.com/internet-anonymity-vs-pseudonymity/>

Pseudonymity

Pseudonymity is a state of disguised identity.

It is a state where an individual hides his/her real identity by using a false name or “pseudonym”.

Some examples of pseudonyms include pen names, nicknames, screen name, and others.

Pseudonyms are widely used in social networks and other virtual communication.

Unlike in anonymity, your own information can be assessed even if it might not [have] the true information about you in it.

Pseudonymity does not guarantee you full concealment of your identity but just a mask to cover yourself.

Source - <http://internet-anonymity.com/internet-anonymity-vs-pseudonymity/>

Anonymity solutions

- Web (http) based
 - Proxies, example: hidemyass.com/proxy, kproxy, hide.me, etc. (some free services, some paid services)
- Hardware based
 - Proxyham, Proxygambit (RasperryPi/Arduino) (\$\$)
 - Anonabox (Tor router) (\$\$)
 - InvizBox (Tor router) (\$\$)
- VPN based
 - List of VPN providers: <https://torrentfreak.com/vpn-anonymous-review-160220/> (\$\$ - can be affordable though)
- Onion router and software based
 - Tor and Tor Browser (free)
 - Whonix (Linux distribution that uses Tor) (free)
 - Tails (another Linux distribution that uses Tor) (free)
 - I2P (distributed) (free)

Tor

- Originally developed by the US Naval Research Laboratory
- Continues to be funded by the US Government
- Open sources under the GPL in 2004
- How it works:

Onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location.

That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous hidden service feature.

Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.

- **Notes:**
 - Does not provide end-to-end encryption
 - Exit nodes can, and have been eavesdropped
 - New board of directors in July 2016...

Tor Browser

- Pre-configured and security hardened Mozilla Firefox ESR distribution designed specifically for Tor
- Automatically starts Tor background processes and routes traffic through the Tor network
- Upon termination of a session the browser deletes privacy-sensitive data such as HTTP cookies and the browsing history
- Tor Browser Demo

VPNs

- List of VPN providers:
<https://torrentfreak.com/vpn-anonymous-review-160220/>
- Look for one that supports OpenVPN and token based authentication.
- Cryptostorm.is
 - Provides token based authentication for OpenVPN rather than usernames/passwords
 - Users can buy tokens from reseller for layered anonymity
 - Can purchase tokens using PayPal, Bitcoin, etc.
 - Pre-created OpenVPN configuration files:
 - https://github.com/cryptostorm/cryptostorm_client_configuration_files

OpenVPN Demonstration

Questions