

A LONG LIST OF ONLINE CRIMES, TOXIC BEHAVIOR AND POLITICAL BEHAVIOR.

1. **Cyberbullying and Harassment**

- Cyberbullying: Repeated online harassment or intimidation aimed at an individual.
- Trolling: Deliberately provoking or upsetting people by posting inflammatory comments.
- Doxxing: Publishing private information about someone online without consent.
- Stalking: Repeatedly contacting or following someone online in a manner that causes fear or distress.
- Online Shaming: Publicly humiliating someone online, usually on social media, to harm their reputation.
- Impersonation: Pretending to be someone else online to deceive or harm others.

2. **Hate Speech and Discrimination**

- Hate Speech: Inciting violence, hatred, or discrimination against a group based on race, religion, ethnicity, gender, sexual orientation, etc.
- Racist or Sexist Remarks: Making derogatory comments aimed at individuals or groups based on their race or gender.
- Misogyny: Expressing contempt or hatred towards women, often leading to online harassment.
- Homophobia or Transphobia: Targeting individuals or groups based on their sexual orientation or gender identity.

3. **Privacy Violations**

- Phishing: Fraudulently obtaining sensitive information (passwords, credit card details) by posing as a trustworthy entity.
- Data Breaches: Unauthorized access to private data from individuals, companies, or governments.
- Identity Theft: Stealing personal information and using it to impersonate someone for financial gain or fraud.
- Spyware: Installing software that secretly monitors or records user activities.
- Tracking without Consent: Using cookies, pixels, or other tools to track user behavior without their consent.
- Deepfakes: Using AI to create realistic but fake videos or images to deceive or manipulate.

4. **Financial Fraud and Scams**

- Online Scams: Tricking users into giving money or personal information through fraudulent schemes (e.g., Nigerian prince scams, lottery scams).
- Investment Fraud: Convincing people to invest in fake or pyramid schemes.
- Ransomware: Infecting a computer with a virus that locks data, demanding payment for its release.
- Credit Card Fraud: Stealing credit card information and making unauthorized transactions.
- Fake Crowdfunding: Setting up fake crowdfunding campaigns to steal donations from well-meaning people.

5. **Intellectual Property and Copyright Violations**

*This list is the result of desktop research.
This document does not pretend to be complete nor to be 100% accurate.
Compiled by Stefan De Greef and for use only in combination with the project I AM REAL®
Contact: stefan.greyhead@gmail.com*

A LONG LIST OF ONLINE CRIMES, TOXIC BEHAVIOR AND POLITICAL BEHAVIOR.

- Piracy: Distributing or downloading copyrighted material (music, movies, software) without permission.
 - Plagiarism: Stealing and publishing someone else's intellectual property as your own, such as written work, art, or research.
 - Trademark Infringement: Using a protected logo, brand, or name without permission.
 - Patent Theft: Copying or illegally distributing patented products or ideas.
 - Counterfeiting: Selling fake goods under the guise of authentic products.
- 6. Misuse of Platforms and Services**
- Spam: Sending unsolicited messages, often in bulk, for advertising purposes.
 - Clickbait: Using misleading headlines or links to trick users into clicking on a webpage.
 - Astroturfing: Creating fake reviews, comments, or testimonials to manipulate public opinion.
 - Fake News: Spreading deliberately false information for political or financial gain.
 - Vote Manipulation: Tampering with online voting systems or polls to skew results.
 - Sockpuppetry: Creating multiple fake accounts to manipulate discussions, influence public opinion, or deceive others.
- 7. Hacking and Cybercrime**
- Hacking: Gaining unauthorized access to computer systems, networks, or devices.
 - Denial of Service (DoS) Attacks: Overloading a website or network with traffic to take it offline.
 - Distributed Denial of Service (DDoS): Coordinating a network of computers to launch a larger-scale attack on a service or website.
 - SQL Injection: Exploiting vulnerabilities in a website's database to steal information or alter records.
 - Botnets: Controlling multiple devices to carry out coordinated attacks or spam campaigns.
 - Malware Distribution: Spreading viruses, worms, or trojans to damage or steal information from computers or networks.
- 8. Child Exploitation**
- Child Pornography: Producing, distributing, or consuming sexually explicit material involving minors.
 - Grooming: Building relationships with minors online with the intent to exploit them sexually or for other illegal purposes.
 - Child Trafficking: Using the internet to recruit, exploit, or sell minors for illegal activities.
- 9. Radicalization and Extremism**
- Terrorist Recruitment: Using online platforms to recruit individuals for terrorist activities.
 - Inciting Violence: Encouraging others to commit acts of violence or terrorism.
 - Promoting Extremist Ideologies: Spreading radical views that encourage division, violence, or hatred towards certain groups.
- 10. Online Pornography-Related Issues**
- Revenge Porn: Sharing explicit images or videos of someone without their consent.

A LONG LIST OF ONLINE CRIMES, TOXIC BEHAVIOR AND POLITICAL BEHAVIOR.

- Non-consensual Deepfake Pornography: Using AI-generated deepfakes to create and distribute fake pornographic content without someone's consent.
 - Obscene Material: Distributing illegal or obscene content, including extreme or violent pornography.
- 11. Political and Election Interference**
- Misinformation Campaigns: Spreading false information to influence election outcomes.
 - Fake Accounts in Politics: Creating fake accounts to promote political agendas, manipulate discussions, or influence voters.
 - Election Hacking: Tampering with election systems to alter results or steal sensitive voter data.
 - Foreign Interference: Using online platforms to meddle in another country's politics or elections.
- 12. Disruptive and Dangerous Challenges**
- Viral Challenges: Encouraging participation in dangerous or harmful activities (e.g., Tide Pod Challenge, Blue Whale Challenge).
 - Encouraging Self-Harm: Promoting suicide, self-harm, or other dangerous behaviors online.
 - Swatting: Making a false emergency call to send law enforcement or SWAT teams to someone's home.
- 13. Manipulation and Psychological Exploitation**
- Gaslighting: Manipulating someone to doubt their perceptions or beliefs, often for personal or political gain.
 - Catfishing: Pretending to be someone else online to deceive people, often for romantic or financial purposes.
 - Emotional Blackmail: Using threats or emotional manipulation to control or extort others online.
- 14. Illegal Online Markets**
- Dark Web Transactions: Engaging in illegal transactions for drugs, weapons, or human trafficking through the dark web.
 - Selling Stolen Goods: Using online platforms to sell stolen items.
 - Fraudulent Online Marketplaces: Setting up fake e-commerce websites to steal money or information from users.
- 15. Obstruction of Justice and Law Enforcement**
- Tampering with Evidence: Destroying or altering online data to hinder investigations.
 - Threatening Witnesses: Using the internet to threaten or intimidate witnesses involved in legal proceedings.
 - Avoiding Law Enforcement: Teaching or helping others to evade law enforcement through encryption, VPNs, or other means.