
Global Certificate in Cyber Psychology

Online Identity and Self-Presentation

Avatar: A digital representation of a user in a virtual environment, often customizable to reflect the user's desired online identity.

Catfishing: The act of creating a fake online identity to deceive or manipulate someone, often with the intention of starting a romantic relationship.

Cyberbullying: The use of digital communication tools, such as social media or messaging apps, to harass, intimidate, or threaten someone.

Cyberstalking: The repeated and unwanted online pursuit of an individual, often with malicious intent.

Digital footprint: The trail of data that individuals leave behind as they use digital technologies, including social media, search engines, and online forums.

Echo chamber: An online environment in which users are exposed only to ideas and opinions that align with their own, often leading to polarization and a lack of critical thinking.

Flaming: The act of sending hostile or insulting messages to someone online, often with the intention of provoking a reaction.

FOMO (Fear of Missing Out): A feeling of anxiety or insecurity that arises from the perception that others are having more exciting or fulfilling experiences.

Grooming: The act of building a relationship with a child or vulnerable individual online with the intention of exploiting them sexually or otherwise.

Hashtag: A word or phrase preceded by the "#" symbol, used on social media to categorize and search for related content.

Internet trolling: The act of posting inflammatory or provocative messages online with the intention of causing upset or conflict.

Memes: Cultural ideas, behaviors, or styles that are transmitted and imitated online, often in the form of images or videos.

Online disinhibition effect: The phenomenon in which individuals behave differently online than they would in face-to-face interactions, often due to a lack of social cues and accountability.

Online persona: The digital identity that individuals present to others online, often through social media

profiles or online communities.

Phishing: The act of sending fraudulent emails or messages that appear to be from a trustworthy source, often with the intention of obtaining personal information or installing malware.

Privacy settings: The options provided by social media platforms and other digital tools that allow users to control who can see their content and personal information.

Sexting: The act of sending sexually explicit messages or images via digital communication tools.

Shadow profile: A collection of data about an individual that is compiled by a social media platform or other digital service, often without the individual's knowledge or consent.

Slactivism: The act of supporting a cause or movement through digital means, often without taking any real-world action.

Sock puppet: A fake online identity created by an individual to deceive or manipulate others, often used for trolling or other malicious purposes.

Troll farm: A coordinated group of individuals who are paid to create and disseminate fake news or propaganda online, often with the intention of influencing public opinion.

Virtue signaling: The act of publicly expressing opinions or beliefs in order to signal one's moral superiority or social justice bona fides, often without taking any real-world action.

VPN (Virtual Private Network): A technology that allows users to connect to the internet through a secure, encrypted connection, often used to protect privacy and bypass internet censorship.

White hat hacker: An ethical hacker who uses their skills to identify and report vulnerabilities in digital systems, often hired by organizations to test their security.

Zoombombing: The act of disrupting a Zoom meeting or other video conferencing session by sharing inappropriate content or taking control of the screen.