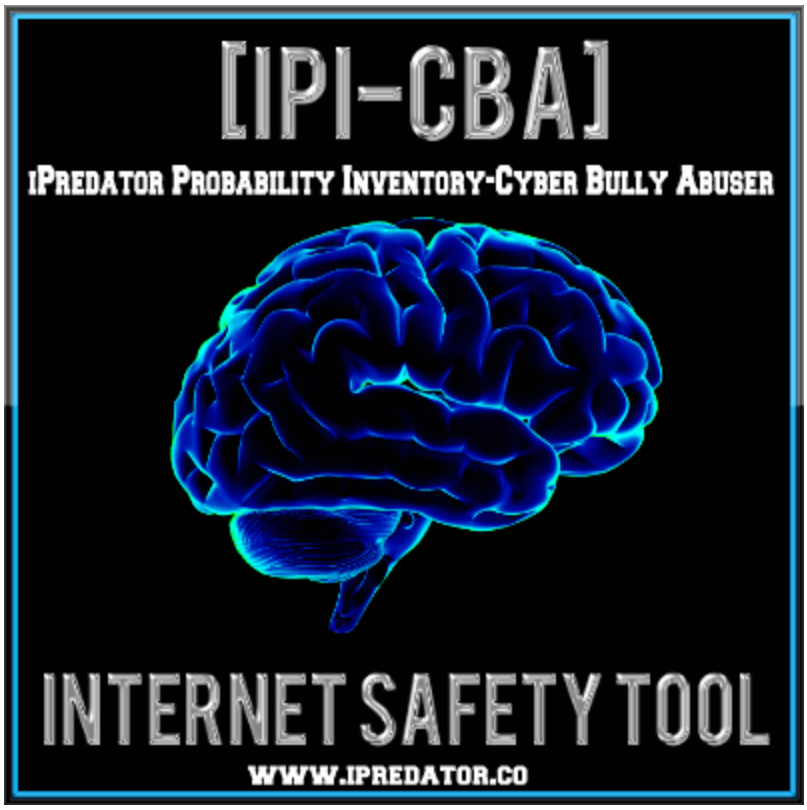
IPI-CBA

iPredator Probability Inventory - Cyberbully Abuser

Michael Nuccitelli, Psy.D.
347-871-2416 New York City, New York
www.ipredator.co



iPredator Probability Inventory - Cyberbully Abuser (IPI-CBA)

The iPredator Probability Inventory - Cyberbully Abuser is a 110-question diagnostic, education, assessment and data collection tool designed to investigate a minor's online probability and potential to intimidate, humiliate and taunt other children engaging in online harassment and cyber bullying. A parent, primary caregiver and school official or pediatric professional complete the IPI-CBA for children, and adolescents ages 6-18.

Once completed, the IPI-CBA score, ranging from 0-110, represents the vulnerability and risk potential of a child becoming a cyberbully abuser or cyberbully bystander. The IPI-CBA can be used as both a cyberbullying assessment tool for children and a data collection instrument for parents and educators investigating cyberbullying episodes involving their child or student.

Like the IPI-CB, the IPI-CBA investigates the knowledge and understanding parents and/or educators have relevant to investigating the cyber bully abuser. The IPI-CBA also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-CBA DIRECTIONS

1. The time required to complete the IPI-CBA inventory averages 60-90 minutes.

2. To complete the checklist, you are required to respond to each statement with 1 of 4 choices as follows:

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

3. Only answer "Yes" or "No" to statements you are positive about or almost certain.

4. If there is a question you do not understand, respond with choice D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

5. If there is a question that does not apply to you or the subject being queried, respond with choice D. DNA__ (Does Not Apply, Not Applicable, Not Relevant). For example, if a checklist statement addresses mobile devices, but you do not own a mobile device, you would respond with choice DNA__.

6. Please provide a response to each question with 1 of the 4 responses before calculating your final score. All questions have been designed to make scoring easy to compile. Simply add up your correct responses (+1) along with (+1) for your D. DNA__ responses and compare your score to the scoring key including in this file.

7. Prior to taking the checklist, please review the following two definitions and refer to them if needed. The definition of Information and Communications Technology (ICT) and iPredator are as follows:

ICT: Information and Communications Technology (ICT) is an umbrella term used to define any electronic or digital communication device or application used to obtain, exchange or disseminate information. ICT stresses the role of unified communications and the integration of telecommunications, which enable users to create access, store, transmit and manipulate information.

ICT consists of all forms of telecommunication, information technology, broadcast media, audio and video processing, transmission and network-based control and monitoring functions. Information and Communications Technology (ICT) is a concept incorporating all electronic and digital forms of communication.

iPredator: A child, adult, group or nation who, directly or indirectly, engages in exploitation, victimization, stalking, theft or disparagement of others using Information and Communications Technology (ICT.) iPredators are driven by deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by economic status, race or national heritage.

iPredator is a global term used to distinguish anyone who engages in criminal, deviant or abusive behaviors using Information and Communications Technology (ICT.) Whether the offender is a cyberbully, cyberstalker, cyber harasser, cybercriminal, online sexual predator, internet troll, online child pornography consumer or cyber terrorist, they fall within the scope of iPredator. The three criteria used to define an iPredator include:

I. A self-awareness of causing harm to others, directly or indirectly, using ICT.
II. The intermittent to frequent usage of Information and Communications Technology (ICT) to obtain, exchange and deliver harmful information.
III. A general understanding of Cyberstealth used to engage in criminal or deviant activities or to profile, identify, locate, stalk and engage a target.

Unlike human predators prior to the Information Age, iPredators rely on the multitude of benefits offered by Information and Communications Technology (ICT.) These assistances include exchange of information over long distances, rapidity of information exchanged and the infinite access to data available. Malevolent in intent, iPredators rely on their capacity to deceive others using Information and Communications Technology (ICT) in an abstract electronic universe.

"*All my checklists and inventories are designed to assess the subject's internet safety acumen, cyber-attack awareness, cyber security practices and general understanding of knowing how to protect oneself in today's digital device environment. Scoring well does not require the respondent to be an advanced information technology professional. If anything, being advanced in electronic devices can give some a false sense of security. Few people score 95% and higher on their first attempt as we are all living at the beginning of a new paradigm called, the Information Age".* Michael Nuccitelli Psy.D., iPredator Inc.

IPI-CBA

Child's Gender: Male___ Female___
Age: Child (6-9) ___ Tween (10-13) ___ Teen (14-18) ___
Average Daily Online Activity: 0-1Hours ___ 1-3 Hours ___ 3+ Hours ___ 5+ Hours ___

ICT = Information and Communications Technology

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

1. Are you confident the minor has not been suspected of direct or indirect cyberbullying (a.k.a., cyberbullying by proxy) attacks?

2. Is the minor discouraged from sending angry or taunting messages online?

3. Is the minor encouraged to discuss cyberbullying issues with adults and loved ones if they are cyberbullying others or being cyberbullied?

4. Are you confident the minor has not been suspected of teasing others using instant messaging or harassment by text messages?

5. Would you or a trusted adult contact the minor's school to resolve online harassment, cyberbullying events or allegations?

6. Are you or a trusted adult positive the minor is not using email messages or chatrooms to vent their anger in a way that hurts others?

7. Would you or a trusted adult join or encourage a PTA Board at the minor's school on cyberbullying?

8. Are you confident the minor has not been suspected of confiscating or damaging another minor's belongings or online identity?

9. Are you confident the minor has not harassed or teased others online?

10. Are you confident the minor has not flamed (a provoking message) others online?

11. Are you confident the minor has not been upset with someone online and sought retribution offline?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

12. Are you confident the minor has not been suspected threatening, embarrassing or teasing others online?

13. Are you confident the minor has not verbalized or posted negative comments online about teachers or students at school?

14. Are you confident the minor has not been suspected of sending or posting mean messages about others based on race, gender, religion or physical attributes?

15. Are you confident the minor has not been suspected of teasing others about their physical attributes?

16. Are you confident the minor has not had an online relationship with negative outcomes initiated by the minor?

17. Are you confident the minor has not spread secrets disclosed to them using ICT?

18. Are you confident the minor has not been suspected by adults or accused by other minors of capturing, saving or storing embarrassing information about another minor?

19. Are you confident the minor has not retaliated to online information being spread about them?

20. Are you confident the minor has not engaged in the cyberbullying tactic called "*Text Wars and Text Attacks",* which is when a cyberbully and their friends gang up on the target minor by sending them hundreds of emails or text messages?

21. Does the minor know how to respond if a friend or classmate is being cyberbullied?

22. Are you confident the minor has not been suspected of "*Interactive Gaming Harassment*"?

23. Are you confident the minor has not engaged in the cyberbullying tactic called "*Denigration",* which is when a minor sends posts or publishes cruel rumors, gossip and untrue statements to intentionally damage their reputation or friendships?

24. Are you confident the minor has not been suspected of signing up a minor to pornography or junk marketing lists?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

25. Are you confident the minor has not been suspected of posting or forwarding negative personal communications about a minor?

26. Are you confident the minor has not been suspected of sending threats of harm, intimidation or offensive comments about a minor?

27. Are you confident the minor has not engaged in the cyberbullying tactic called "*Phishing*", which is when a cyberbully manipulates the target minor into revealing their passwords then accesses their accounts?

28. Are you confident the minor has not been suspected of sexting?

29. Are you confident the minor has not been suspected of stealing a minor's password and chatting with others pretending to be the target minor?

30. Are you confident the minor has not sent or received offensive content regarding peers using ICT?

31. Are you confident the minor has not been suspected of consistently teasing others using ICT?

32. Are you confident the minor has not observed the minor being aggressive or hostile to others using ICT?

33. Are you confident the minor would not be a bystander if their friend or classmate was being harassed and teased online?

34. Are you confident the minor does not encourage cyberbullying and online teasing?

35. Are you confident the minor has not engaged in the cyberbullying tactic called "*Exclusion*", which is when a cyberbully invites peers to a social function, but does not invite or discuss the function with the target minor?

36. Are you confident the minor has not shared images or videos to embarrass others using ICT?

37. Does the minor practice "*Digital Citizenship*" and "*Netiquette*" (online manners) with classmates and peers?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

38. Are you confident the minor has not teased others using ICT and reported they are joking?

39. Are you confident the minor has not engaged in the cyberbullying tactic called "*Exposure*", which is when a minor displays, posts or forwards disparaging personal communication, images or video about a target minor online?

40. Have you or a trusted adult sat down with the minor, engaged them in a discussion on cyberbullying and feel confident they do not cyberbully or are partisan to cyberbullying?

41. Are you confident the minor has not been the victim of bullying, cyberbullying or a bystander of cyberbullying?

42. Are you confident the minor has not been suspected of sending embarrassing or suggestive images or videos of a minor using mobile devices?

43. Do you or a primary caregiver know a cyberbully can make threats, share gossip, spread lies and start rumors all from their home computer and mobile device?

44. Are you confident the minor has not been suspected of being verbally abusive and harassing towards another minor while keeping their identity unknown using ICT?

45. Are you confident the minor has not disclosed negative personal information about other minors at websites, forums or in chatrooms?

46. Are you confident the minor does not lack remorse or feel other minors deserve having embarrassing personal information posted online about them?

47. Are you confident the minor has not been suspected of posting sexual information of other minors using ICT?

48. Are you confident the minor has not withdrawn from their favorite activities by spending more time using ICT not typical of minor and teen development?

49. Are you confident the minor has not withdrawn from friends and family members by spending more time using ICT without explanation?

50. Are you confident the minor has not experienced a loss of appetite preferring to engage in ICT usage not typical of minor and teen development?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

51. Are you confident the minor has not engaged in the cyberbullying tactic called "*E-mail Threats and Dissemination*", which is when a minor inspires fear in the target minor by communicating threats using email?

52. Are you confident the minor has not had a drastic change in grades due to spending more time using ICT not typical of minor and teen development?

53. Are you confident the minor has not experienced a change in attitude, seems upset and spends more time using ICT not typical of minor and teen development?

54. Are you confident the minor has not recently shown aggressive or dominant behavior using ICT without explanation or typical of minor and teen development?

55. Are you confident the minor has not engaged in the cyberbullying tactic called "*Imping*", which is when a cyberbully impersonates the target minor and makes unpopular comments on social sites and in chatrooms?

56. Are you confident the minor has not engaged in the cyberbullying tactic called "*Interactive Gaming Harassment*", which is when a minor verbally abuses another minor within gaming environments?

57. Do you or a trusted adult know how to effectively advise the minor if he or she has "*flamed*" (a provoking message) other minors online?

58. Do you or a trusted adult know how to respond if the minor feels satisfied or vindicated from cyberbullying or teasing other minors using ICT?

59. If the minor has been a victim of cyberbullying, are you or a trusted adult aware the minor may experience depression and begin to isolate from their peers and loved ones?

60. Are you or a trusted adult prepared if the minor voices anger about being teased online and wanting to strike back seeking revenge?

61. Are you or a trusted adult aware if a cyberbully victimizes the minor, he or she may cyberbully others?

62. Are you confident the minor has not engaged in the cyberbullying tactic called "*Pornography and Marketing List Inclusion*", which is when a cyberbully signs their target up to numerous pornography or junk marketing lists?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

63. Is it better for the minor to ignore contacts from a cyberbully and speak with a trusted adult, parent or teacher?

64. Is it true that cyberstalking is a dangerous form of cyberbullying and both you and the minor understand the difference?

65. Are you confident the minor has not been suspected of "*Denigration*", which is when a minor sends or posts cruel rumors about a target minor to intentionally damage their reputation or friendships?

66. Are you confident the minor has not engaged in the cyberbullying tactic called "*Griefing*", which is when a minor causes frustration to the target minor and his/her peers by not following the rules of an interactive online video game?

67. Is the minor cautious when posting personal information online?

68. Do you, a trusted adult or the minor understand and monitor their "*Digital Footprint*"?

69. Are you confident the minor has not shared confidential information about an ex-friend, ex-partner or enemy using ICT?

70. Are you confident the minor has not engaged in the cyberbullying tactic called "*Password Theft & Lockout*", which is when a minor steals the target minor's password and begins to chat with other people, pretending to be the target minor?

71. Are you confident the minor does not share other minor's online images and videos with online strangers?

72. Does the minor understand the basic concepts of "*Digital Reputation*" and practice digital citizenship?

73. Does the minor know images and videos they post online can remain in cyberspace for years?

74. Does the minor know information shared or posted online may be impossible to delete?

75. Are you confident the minor does not have a mobile device with sensitive information about other minors?

76. Are you confident the minor has not been suspected by adults or accused by other minors of sexting?

77. Does the minor know how their own or another minor's personal information can go viral?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

78. Does the minor know negative information they post or share about others online will be reflected in their digital footprint?

79. Does the minor know images and videos they share about others online can be reposted multiple times and downloaded by online strangers?

80. Do you or a trusted adult educate the minor on the types of information that can be harmful to other minor's digital reputation?

81. Do you or a trusted adult take steps to ensure the minor does not post or share information that is damaging to another minor's digital reputation?

82. Do you or a trusted adult respectfully monitor what information the minor posts online?

83. Does the minor practice good behavior online and in chatrooms?

84. Do you enter the minor's personal information into search engines to track is they have been cyberbullying others or being cyberbullied?

85. Do you respectfully check the minor's email and social media profiles to track signs of cyberbullying?

86. Are you confident the minor has not engaged in sexting involving other peers and passed this information to other peers?

87. Do you or a trusted adult spend time with the minor educating them on their digital reputation?

88. Does the minor know the content they share or post online about others can be reposted hundreds of times and end up being viewed by online strangers?

89. Are you confident the minor has not engaged in the cyberbullying tactic called "*Voting/Polling Booths*", which is when a minor uses voting/polling website to vote online in categories about the target minor that are highly embarrassing?

90. Are you or a trusted adult confident the minor has been educated on how to practice "*Netiquette*"?

91. Does the minor know iPredators target minors using kindness and understanding and seek to disclose personal information about their friends and other minors?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

92. Are you confident the minor has not teased, harassed or joked with others using ICT and became angry?

93. Are you confident the minor has not teased, harassed or joked with others using ICT for revenge?

94. Are you confident the minor has not teased, harassed or joked with others using ICT and appeared satisfied or proud?

95. Does the minor know teasing, harassing or joking about others online is all forms cyberbullying?

96. Does the minor know teasing, harassing or joking about others offline often leads to cyberbullying?

97. Does the minor know teasing, harassing or joking about others using ICT by accident is cyberbullying?

98. Does the minor know teasing, harassing or joking about others using ICT to be more popular is cyberbullying?

99. Does the minor know teasing or joking about the physical attributes of another minor using ICT is cyberbullying?

100. Does the minor know teasing or joking about the sexual orientation of another minor using ICT is cyberbullying?

101. Does the minor know teasing, harassing or joking about others using ICT motivated by "righting wrongs" is cyberbullying?

102. Are you confident the minor does not think teasing, harassing or joking about others online makes them more popular or liked by other minors they find attractive?

103. Are you confident the minor does not spend long hours on the computer or using their mobile devices in private?

104. Are you confident the minor does not close their computer or turn off their mobile device when you or a trusted adult enters the room?

105. Are you confident the minor is not secretive about their internet activities?

A. Y__ (Yes, Agree, True)
B. N__ (No, Disagree, False)
C. IDK__ (I Do Not Know, I Did Not Know, I Am Unsure)
D. DNA__ (Does Not Apply, Not Applicable, Not Relevant)

106. Are you confident the minor is not getting behind in school or seems preoccupied because of the time they spend online?

107. Are you confident the minor has not been suspected of engaging in cyberbullying by proxy, which is enlisting friends to disparage a target minor online?

108. Are you confident the minor has not engaged in the cyberbullying tactic called "Happy Slapping", which is when the target minor is physically attacked or embarrassed in person and an accomplice video records or takes pictures of the incident?

109. Are you confident the minor has not sent an email from minor's email accounts without their consent or knowledge?

110. Are you confident the minor has not been suspected of impersonating another minor using Twitter, online postings or in chatrooms?

CORRECT RESPONSE TO EVERY QUESTION IS A. Y__ (Yes, Agree, True)

Yes Answers __ No Answers __ I Do Not Know__ Does Not Apply__

Correct Responses__+ Does Not Apply Responses__= IPI Score__

Michael Nuccitelli, Psy.D.
NYS Licensed Psychologist & iPredator Construct Author
iPredator Inc. New York, USA
347-871-2416 info@ipredatorinc.com
www.ipredator.co

Note: The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. *"I Do Not Know"* & *"No"* responses should be addressed immediately with a plan of action. Although obtaining a score of 90 or higher indicates a minimal probability of a successful cyber-attack, it is still crucial to be alert and prepared to defend against iPredators, ex-partners and those who would seek to destroy your digital reputation.

As Information and Communications Technology expands, it will become increasingly important to manage and monitor cyber-attack prevention, digital citizenship and digital reputation.

(link for web page scoring key)
Internet Safety Tool Scoring Keys Page: https://www.iPredator.co/scoring-keys/

Given the rapid expansion and advancements in ICT, it is recommended to complete this inventory on a quarterly basis and more frequently if an iPredator is suspected of engaging in a possible cyber-attack. To achieve optimal cybercrime, cyber-attack and/or cyber assault prevention, the goal is to score in the upper 10%-15% of all the IISC assessments. Cyberspace is a non-physical abstract electronic universe. The toll it can take on vulnerable and/or ignorant online users are very real and can range from frustrating to deadly.

IISC SCORE DEFINITION

IISC Score: Upon completion of any of the IISC assessments, the respondent will have a final score ranging from 0-75, 0-110 or 0-330 depending on the IISC assessment. In this formula, the score represents the risk potential and vulnerability of the ICT user, the business or the subject being queried from being targeted by a cyberbully, cyberstalker, cybercriminal, nefarious corporate competitor or online sexual predator.

IPI SCORING KEY

IPI Score: (1-10)
Category: Guaranteed Cyberbully
Risk Potential: Alarmingly High
iPredator Involvement: Certain
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Urgent Attention Required

IPI Score: (11-29)
Category: Prime Cyberbully
Risk Potential: High
iPredator Involvement: Almost Certain
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Immediate Attention Required

IPI Score: (30-39)
Category: Probable Cyberbully
Risk Potential: Moderately High
iPredator Involvement: Involvement Likely
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Immediate Attention Strongly Recommended

IPI Score: (40-55)
Category: Likely Cyberbully
Risk Potential: Moderate
iPredator Involvement: Involvement Suspected
Intervention Plan: Create and Implement an iPredator Prevention Plan
Level of Urgency: Immediate Attention Recommended

IPI Score: (56-69)
Category: Possible Cyberbully
Risk Potential: Moderate
iPredator Involvement: Involvement Possible
Intervention Plan: Increase iPredator Protection & Prevention Strategies
Level of Urgency: Immediate Attention Suggested

IPI Score: (70-84)
Category: Low Probability Cyberbully & Bystander
Risk Potential: Mild
iPredator Involvement: Possible, but Unlikely
Intervention Plan: Continue iPredator Protection & Prevention Strategies
Level of Urgency: Not Urgent, Important to Address Below 80

IPI Score: (90-110)
Category: Minimal Probability Cyberbully & Bystander
Risk Potential: Minimal
iPredator Involvement: Unlikely
Intervention & Education Plan: Consider Educating Others
Level of Urgency: 0%, All iPredator Issues Addressed

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist and cyber criminology consultant. He completed his doctoral degree in clinical psychology from Adler University in 1994. In 2010, Dr. Nuccitelli published his dark side of cyberspace concept called "iPredator." In November 2011, he established iPredator Inc., offering educational, investigative, and advisory services involving online assailants, cyber-attack targets, dark psychology and internet safety. Dr. Nuccitelli has worked in the mental health field over the last thirty-plus years and he has volunteered his time helping cyber-attacked victims since 2010. His goal is to reduce victimization, theft, and disparagement from iPredators.

In addition to aiding citizens & disseminating educational content, Dr. Nuccitelli's mission is to implement a permanent national educational and awareness online safety campaign with the help of private, state, and federal agencies. He is always available, at no cost, to interact with online users, professionals, and the media. To invite Dr. Nuccitelli to conduct training, media engagements, educational services, or consultation, please call him at (347) 871-2416 or via email at drnucc@ipredatorinc.com.

- LinkedIn: Michael Nuccitelli, Psy.D.
- Twitter: @TheiPredator
- Facebook Page: The iPredator
- Facebook: Michael Nuccitelli
- Pinterest: iPredator
- Tumblr: iPredator
- Instagram: #drnucc