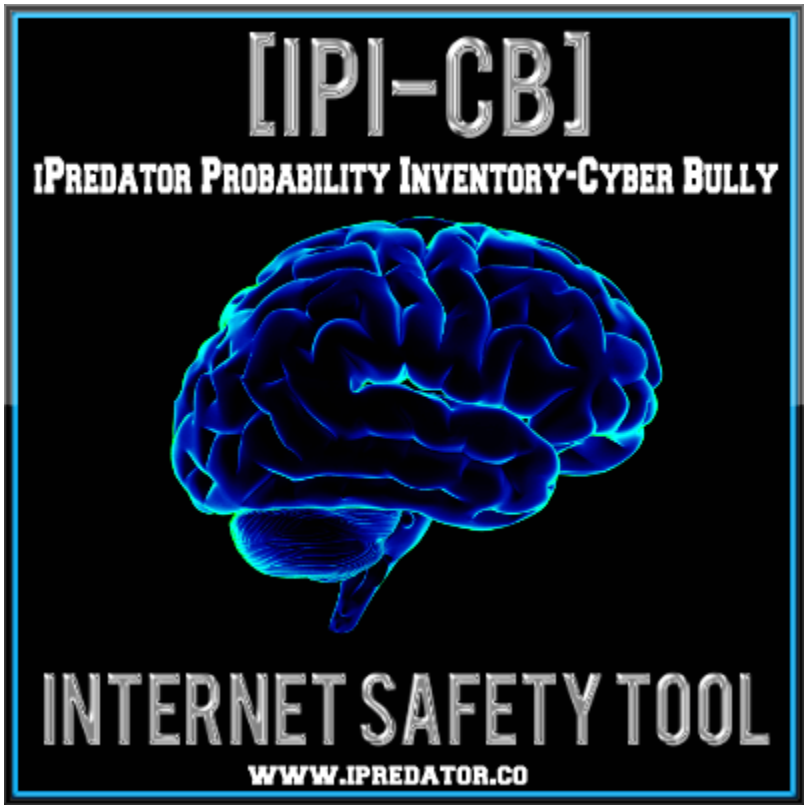
IPI-CB

iPredator Probability Inventory – Cyberbully

Michael Nuccitelli, Psy.D.
www.ipredator.co



iPredator Probability Inventory – Cyberbully (IPI-CB)

The iPredator Probability Inventory-Cyberbully is a 110-question diagnostic, education, assessment and data collection tool designed to investigate a child or adolescent's online preparedness, vulnerability and risk potential for being cyber bullied and/or harassed. Just as all the IPI assessment collection inventories, the IPI-CB focuses on the child's relationship to ICT, their knowledge base of malevolent and nefarious users, environmental aspects influencing their Information and Communications Technology (ICT) activities and their practice of the behavioral actions necessary for internet safety and preparedness if cyber attacked.

The IPI-CB also explores parental and support system cyberbully protection and prevention tactics employed by loved ones and school officials. A parent, primary caregiver, educator or pediatric professional completes the IPI-CB for children and adolescents ages 6-17. Once completed, the IPI score, ranging from 0-110, represents the preparedness, vulnerability and risk potential of the child becoming a cyberbully target, cyberbully abuser or cyberbully bystander. The IPI-CB can be used as both a cyberbullying prevention tool for children and a data collection instrument for parents and educators investigating cyberbullying episodes involving their child or student.

IPI-CB DIRECTIONS

1. The time required to complete the IPI-CB 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 seemingly 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-CB

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 ___

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. Is the minor capable of not becoming overly distressed from opening emails or reading online information about them that is negative, false or disparaging?

2. Is the minor familiar with the cyberbullying tactic called "*Pseudonym Stealth*", which is when a cyberbully makes threatening or disparaging comments, but can hide whom they are?

3. Is the minor actively encouraged to tell a trusted adult if they are teased, harassed or taunted online?

4. Is the minor familiar with the cyberbullying tactic called "*Instant Messaging Attacks*", which is when a cyberbully uses instant messaging or text messaging to taunt or harass another minor?

5. Would you or a trusted adult use the minor's school as a resource to resolve cyberbullying events, despite the minor fearing escalated cyberbullying from parental involvement?

6. Are you or a trusted adult 100% positive the minor has not, and would not, use chatrooms to vent their anger in a way that would be defined as cyberbullying?

7. Would you encourage, join or support PTA education, at the minor's school, about bullying and cyberbullying, despite the minor fearing escalated cyberbullying from adult involvement in their affairs?

8. Do you or a trusted adult regularly discuss bullying & cyberbullying with the minor whether they are being cyberbullied or not?

9. Is the minor familiar with 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?

10. Does the minor know how to ignore being harassed or teased online by a cyberbully without becoming overly distressed?

11. Are you, an educator or primary caregiver confident the minor has not been flamed (a provoking message) online and would become overly distressed?

12, Are you, an educator or primary caregiver confident the minor, has not, and would not, become sullen or angry with someone harassing or teasing them 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)

13. Are you, an educator or primary caregiver confident the minor has not, and would not, become overly distressed from being threatened, embarrassed or teased online?

14. Are you, an educator or primary caregiver confident the minor has not, and would not, become negative about school due to being teased or harassed by classmates?

15. Is the minor familiar with the cyberbullying tactic called "*Exposure*", which is when a cyberbully displays, posts or forwards personal communication, images or video about the target minor online?

16. Are you, an educator or primary caregiver confident the minor has not, and would not, keep secret being teased or embarrassed online by someone you or a trusted adult does not know?

17. Are you, an educator or primary caregiver confident the minor has not, and would not, have an online relationship involving negative outcomes?

18. Are you, an educator or primary caregiver confident the minor has not had secrets they have disclosed spread by others using ICT?

19. Has anyone captured, saved or stored embarrassing information about the minor using ICT?

20. Are you, an educator or primary caregiver confident the minor has not, and would not, retaliate to online information being spread about them using ICT?

21. Are you, an educator or primary caregiver confident the minor has not been harassed or teased online due to their physical attributes?

22. Does the minor know how to respond if a friend or classmate is being cyberbullied and the importance of telling a trusted adult?

23. Does the minor know whom, when and how to report a bully or cyberbully and the importance of telling a trusted adult is they are unsure?

24. Are you, an educator or primary caregiver confident the minor has not received online offensive content regarding peers or classmates and kept it a secret?

25. Are you, an educator or primary caregiver confident the minor has not been teased or harassed online, became upset and wanted to behave in a self-destructive manner?

26. Have you, an educator or a primary caregiver observed the minor being aggressive and/or mean to others online?

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)

27. Are you, an educator or primary caregiver confident the minor has not, and would not, be a bystander if their classmates were being harassed and teased online?

28. Does the minor know what actions and behaviors encourage a cyberbully?

29. Is the minor familiar with the cyberbullying tactic called "*E-mail Threats and Dissemination*", which is when a cyberbully inspires fear in the target minor by communicating threats that may be direct or implied using email?

30. Does the minor know personal images and videos they share online can be used to embarrass them by cyberbullies and ex-friends?

31. Does the minor practice digital citizenship (online manners) and understand the importance of "netiquette?"

32. Does the minor understand what to do if cyberbullied and threatened to keep it a secret or more teasing and taunting will follow?

33. Are you, an educator or primary caregiver confident the minor has not posted or shared information, images or video that he or she has been teased about online?

34. Have you or a trusted adult engaged the minor in a discussion on cyberbullies and feel confident they are prepared if they are cyberbullied?

35. Are you, an educator or primary caregiver confident the minor has never been the victim of cyberbullying due to their sexual orientation or race?

36. Do you, a trusted adult and the minor know cyberbullies will disseminate embarrassing or suggestive photos online and not disclose their identity?

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

38. Is the minor aware a cyberbully can be verbally abusive and harassing while their identity remains unknown or claim to be someone they are not?

39. Is the minor psychologically prepared if a cyberbully discloses unfavorable information about them on websites, forums and in chatrooms?

40. Do you and the minor have a crisis plan if a cyberbully spreads embarrassing personal information about the minor?

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)

41. Do you and the minor know what steps to take if a cyberbully spreads sexually themed rumors the minor online?

42. Are you, an educator or primary caregiver confident the minor has not become withdrawn from their favorite activities due to being cyberbullied by peers?

43. Are you, an educator or primary caregiver confident the minor has not withdrawn from friends and family members due to their online activities?

44. Are you, an educator or primary caregiver confident the minor has not experienced a loss of appetite due to their online activities?

45. Are you, an educator or primary caregiver confident the minor has not shown a recent dislike or fear of going to school due to their online activities?

46. Are you, an educator or primary caregiver confident the minor has not had a drastic change in grades due to their online activities?

47. Are you, an educator or primary caregiver confident the minor has not experienced a change in attitude and seems depressed due to their online activities?

48. Are you, an educator or primary caregiver confident the minor has not recently shown aggressive or dominant behavior due to their online activities?

49. Are you, an educator or primary caregiver confident the minor has not recently shown a pattern of escalating agitation due to their online activities?

50. Are you, an educator or primary caregiver confident the minor has not engaged in cyberbullying or "*Cyberbullying by Proxy*"?

51. Do you or a trusted adult know how to effectively advise the minor if he or she has been "flamed" (provocative online message) by classmates or peers?

52. Is the minor familiar with the cyberbullying tactic called "Phishing", which is when a cyberbully manipulates the target minor into revealing their passwords then accesses their accounts?

53. If the minor has or ever becomes a victim of cyberbullying, are you or a trusted adult prepared if the minor experiences depression?

54. Are you or a trusted adult educated on cyber bullicide and prepared if the minor voices suicidal thoughts from being cyberbullied?

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)

55. Are you or a trusted adult aware if the minor is cyberbullied, he or she may become self-destructive online that is not always evident offline?

56. Is the minor familiar with the cyberbullying tactic called "*Imping*", which is when a cyberbully impersonates the target minor and makes unpopular comments on social sites and in chatrooms?

57. Does the minor know it is better to ignore contacts from a cyberbully, and tell a trusted adult, as opposed to keeping it secret or cyberbullying others?

58. Does the minor know that cyberstalking is a dangerous form of cyberbullying and can lead to physical assault if he or she does not report the attacks?

59. Is the minor familiar with "*Exclusion*", a bullying and cyberbullying tactic whereby the minor is the only one not invited to online or offline social activities?

60. Is the minor familiar with the cyberbullying tactic called "*Denigration*", which is when a cyberbully sends, posts or publishes cruel rumors, gossip and untrue statements to intentionally damage their reputation or friendships?

61. Is the minor cautious when posting personal information online and understands how information online can easily be distorted?

62. Do you, a trusted adult or the minor know what "*Digital Footprint*" means and how cyberbullies disseminate information about the target minor that negatively affects their digital footprint?

63. Has the minor confirmed they have not shared private or sensitive information to an ex-friend or ex-partner online that is embarrassing?

64. Does the minor practice caution what they disclose to friends met online?

65. Does the minor protect their images and videos from online strangers viewing and downloading them online?

66. Do you, a trusted adult or the minor know what "*Digital Reputation*" means and how to monitor their digital reputation?

67. Does the minor know their images and videos can remain in cyberspace for years and passed around by both friends and adversaries without their consent?

68. Does the minor know information they post or share online may be impossible to delete and can be used against them if a cyberbully acquires the information?

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)

69. Does the minor have a mobile device without information that is embarrassing or private?

70. Does the minor know how "sexting" can be shared with others and may be criminal?

71. Does the minor know how their personal information can go viral without their knowledge or consent?

72. Is the minor familiar with the cyberbullying tactic called "*Interactive Gaming Harassment*", which is when a cyberbully verbally abuses and threatens the target minor within gaming environments?

73. Is the minor familiar with 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?

74. Do you or a trusted adult educate the minor on disseminating information online that is harmful to their digital reputation and can be used by cyberbullies?

75. Is the minor familiar with the cyberbullying tactic called "*Griefing*", which is when a cyberbully habitually and chronically causes frustration to the target minor by not following the rules of an interactive online video game?

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

77. Is the minor familiar with the cyberbullying tactic called "*Password Theft & Lockout*", which is when a cyberbully steals the target minor's password and begins to chat with other people, pretending to be the target minor?

78. Do you or a trusted adult enter the minor's personal information into search engines to track if they are being disparaged by classmates or peers online?

79. Do you or a trusted adult respectfully check the minor's email and social media profiles to track if they are being disparaged online?

80. Are you, an educator or primary caregiver confident the minor has not engaged in sexting?

81. Do you or a trusted adult spend time educating the minor on being cautious about posting personal information using their mobile devices?

82. Is the minor familiar with the cyberbullying tactic called "*Voting/Polling Booths*", which is when a cyberbully uses voting/polling websites to vote online in categories about the target minor that are highly embarrassing?

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)

83. Does the minor know the information they share online can hurt their future and be used by cyberbullies to hurt their reputation?

84. Are you confident the minor has not been teased or harassed online by a cyberbully and began teasing or harassing others other than the cyberbully?

85. Are you, an educator or primary caregiver confident the minor has not been teased or harassed online because of their economic status?

86. Are you, an educator or primary caregiver confident the minor has not been teased or harassed online and felt helpless or hopeless?

87. Does the minor know persistent teasing, harassing or joking about others online is defined as cyberbullying?

88. Does the minor know persistent teasing, harassing or joking about others online for entertainment purposes is cyberbullying?

89. Does the minor know persistent teasing, harassing or joking about others online by accident is cyberbullying?

90. Does the minor know persistent teasing, harassing or joking about others online to impress the opposite sex is cyberbullying?

91. Does the minor know persistent teasing, harassing or joking about others online, motivated by chivalry, is cyberbullying?

92. Does the minor know persistent teasing, harassing or joking about others online, which is motivated by "righting wrongs" is cyberbullying?

93. Is the minor familiar with the cyberbullying tactic called "*Bash Boards*", which is when a cyberbully posts negative and deprecating information about the target minor on online bulletin boards?

94. Is the minor familiar with 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?

95. Is the minor familiar with 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?

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)

96. Are you, an educator or primary caregiver confident the minor is not secretive about their online activities?

97. Are you, an educator or primary caregiver confident the minor is not getting behind in schoolwork due to their online activities or from being targeted by a cyberbully?

98. Are you, an educator or primary caregiver confident the minor has not had someone send a message from his or her personal email account without his or her consent or knowledge?

99. Are you, an educator or primary caregiver confident the minor has not been impersonated by someone else using instant messaging (IM) or text messaging?

100. Are you, an educator or primary caregiver confident the minor has not been persistently teased, harassed or taunted by someone over IM, in chat rooms or using Twitter?

101. Are you, an educator or primary caregiver confident the minor has not been asked by peers or classmates to give them his or her passwords?

102. Are you, an educator or primary caregiver confident the minor has not had a private instant messaging (IM) conversation or e-mail message sent to others without their consent?

103. Are you, an educator or primary caregiver confident the minor has never been embarrassed or frightened by someone changing their social networking site profile or "away" message without their knowledge?

104. Are you, an educator or primary caregiver confident the minor has never had images or information posted about them on a website without their consent?

105. Are you, an educator or primary caregiver confident the minor has not had an internet poll, either over IM or on a website, about them without their permission?

106. Are you, an educator or primary caregiver confident the minor has not had a peer or classmate use information found online to follow, tease, embarrass or harass the minor in person?

107. Are you, an educator or primary caregiver confident the minor has never had someone use a mobile phone to take photos of the minor without their consent?

108. Are you, an educator or primary caregiver confident the minor does not enjoy the anonymity inherent on the internet to say things they would not usually say in real life?

109. Are you, an educator or primary caregiver confident a peer or classmate has not posted malicious information about the minor online?

110. Are you, an educator or primary caregiver confident the minor does not appear angry, fearful or sullen when they shut off their computer or mobile device?

ALL CORRECT RESPONSES TO QUESTIONS ARE A. Y__ (Yes, Agree, True)

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

Correct Responses__+ Does Not Apply Responses__= IPI-CB Score__

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 Target
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 Target
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 Target
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 Target
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 Target
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: Skilled Cyberbully Protection with Low Vulnerability
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: Advanced Cyberbully Protection with Minimal Vulnerability
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, cyberpsychology researcher and online safety educator. In 2009, Dr. Nuccitelli finalized his dark side of cyberspace concept called iPredator. Since 2010, he has advised those seeking information about cyberbullying, cyberstalking, cybercriminal minds, internet addiction and his Dark Psychology concept. By day Dr. Nuccitelli is a practicing psychologist, clinical supervisor and owner of MN Psychological Services, PLLC. After work and on the weekends, he volunteers helping online users who have been cyber-attacked. Dr. Nuccitelli's is always available to interested partied and the media at no cost. The iPredator website and everything created by Dr. Nuccitelli is educational, free and public domain.