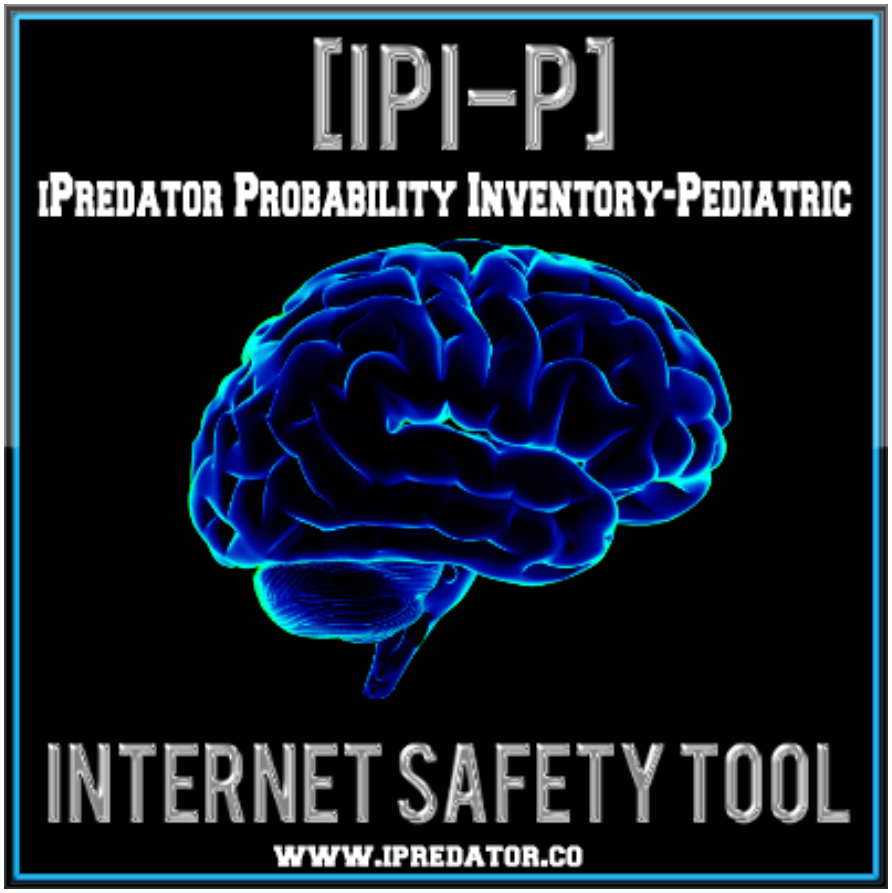
IPI-P

iPredator Probability Inventory - Pediatric

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



iPredator Probability Inventory - Pediatric (IPI-P)

The iPredator Probability Inventory - Pediatric is a 110-question diagnostic, education, assessment and data collection tool designed to investigate a child, adolescent or young adult regarding their online victimization risk potential, cyber-attack awareness and support system involvement.

A parent, family member or pediatric professional completes the IPI-P. Once completed, the IPI score ranging from 0-110 represents the child, adolescent or young adult's preparedness, vulnerability and risk potential of being targeted by an iPredator engaged in cyberbullying, cybercrime, cyberstalking, cyber harassment or trolling for targets to sexually victimize.

The IPI-P investigates these areas problematic to all Information Age children and adolescents. The long-form version of the IPI-P is the IPI-330 is designed for those seeking an exhaustive diagnostic tool with added elements. The IPI-P also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-P DIRECTIONS

1. The time needed to complete the IPI-P inventory averages 60-90 minutes.

2. To complete the checklist, you must 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 ability 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 need 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-P

Child's Gender: Male__ Female__
Age: (6-12) __ (13-14) __ (15-16) __ (17-18) __ (19-21) __
Average Daily Online Activity: 0-1 Hours __ 1-3 Hours __ 3-5 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 child familiar with the two main types of cyber bullying: direct and indirect attacks (aka: cyber bullying by proxy?) YES
2. In the last 90 days, has anyone made a racial, sexist, sexual or derogatory statement about the child's family online? NO
3. In the last 90 days, has anyone posted a lie or false allegation about the child online? NO
4. In the last 90 days, has anyone flamed (angry or provocative message) the child online? NO
5. In the last 90 days, has the child been cyberbullied? NO
6. In the last 90 days, has anyone they know been cyberbullied? NO
7. Has the child sent, posted or received mean messages about others online? NO
8. In the last 6 months, has a friend or enemy spread rumors about them online? NO
9. In the last 6 months, has a friend or enemy disclosed a secret about them online? NO
10. Has the child ever teased or hurt someone online? NO
11. Does the child know what to do if they or a friend is cyberbullied? YES
12. Is the child's address and phone number hidden online from everyone other than trusted adults and/or close friends online? YES
13. Does the child know posting personal information online can hurt their reputation? YES
14. Has the child shared confidential information to a new ex-friend or ex-romantic partner online? NO
15. Is the child careful what they tell others online, which you have verified through discussions or proof? YES
16. Does the child protect their images from strangers viewing them online? YES
17. Does the child have a positive digital reputation? YES
18. Does the child know their images and videos can remain in cyberspace for years? YES
19. Does the child know negative online information about them may be impossible to delete? YES
20. Does the child have a mobile device (i.e. cellphone, smartphone) with information that is embarrassing? NO
21. Does the child know "sexting" may be a criminal act if shared with others? YES

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)

22. Has the child talked about sex with someone they met online? NO
23. Does the child have a social profile set to "public" in their privacy settings? NO
24. Does the child tell friends their passwords? NO
25. Has the child communicated in chat rooms with others they do not know or have not met? NO
26. Has the child text messaged or chatted about sex online with others they do not know? NO
27. Has the child ever been contacted by or conversed with an online stranger? NO
28. Has the child ever met someone in person he or she met online without telling you? NO
29. Has the child ever turned off, logged out or close their computer when you or a loved one walked in? NO
30. Does the child accept on their "buddy" or "friends" lists others they do not know? NO
31. Does the child chat with others they do not know and keep it a secret from you? NO
32. Has the child learned about iPredators, online sexual predators and cyber bullying? YES
33. Does the child know iPredators are usually kind and understanding? YES
34. Does the child know iPredators offer gifts to online users? YES
35. Does the child know iPredators will try to steal their identity? YES
36. Does the child know iPredators create profiles pretending to be their age? YES
37. Does the child know iPredators will ask to add them to their "buddy" or "friends" lists? YES
38. Does the child know peer-to-peer networks (P2P) expose their computer/networks to iPredators? YES
39. Does the child know the best protection from iPredators is being honest and open with their parents and trusted adults? YES
40. Does the child know that most young people sexually abused online are manipulated or coerced into meeting? YES
41. Does the child know to be careful of anyone online who encourages them to lie to their parents or trusted adults? YES
42. Does the child know iPredators look for young people online late at night? YES
43. Does the child have a mobile phone that is password protected in case it is lost or stolen? YES
44. Does the child know how to prevent access to his or her mobile phone? YES
45. Has the child learned about the dangers of GPS location services? YES

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)

46. Does the child know GPS location services allow anyone to know their exact location? YES
47. Does the child know how to install and update their mobile phone security filters, controls and deactivate GPS services when not needed? YES
48. Has the child learned about mobile device and mobile phone safety? YES
49. Does the child know how to install and activate security features on their mobile phone? YES
50. Does the child know and follow his/her school's rules on using mobile phone usage? YES
51. Is antivirus software installed on the child's mobile devices? YES
52. Does the child or his or her close friends regularly visit pornography or dangerous websites? NO
53. Does the child know to never share passwords with loved ones not approved by you or a trusted adult? YES
54. Does the child post their home or mobile phone numbers online? NO
55. Does the child know they can disclose their phone number by Caller ID to others they do not know? YES
56. Does the child know it is good to have many passwords they change often? YES
57. Do friends know the child's computer or mobile phone passwords? NO
58. Does the child visit adult chat rooms and keeps it a secret from you? NO
59. Does the child know what to do if they are sent to a hate, violence or racist website? YES
60. Does the child know about bot software, spyware, keystroke loggers and viruses? YES
61. Does the child know that social sites are frequented by iPredators? YES
62. Does the child share their home or mobile phone numbers in chat rooms? NO
63. Does the child share their contact information at gaming sites or in chat rooms? NO
64. Does the child share their images or videos with others online they have never met? NO
65. Does the child always log off when not using instant messaging or their email? YES
66. Does the child know about the dangers of sharing their full name online? YES
67. Is the child's school website password protected from viewing students? YES
68. Does the child tell their friends about the dangers of sharing personal information online? YES
69. Does the child make sure sites they have joined do not show their personal information? YES
70. Do any of the child's user account or profile names include their full or partial real name? NO

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)

71. Does the child post their full name and/or home address online? NO
72. Does the child know to never give out his or her password to anyone online? YES
73. Does the child discourage friends from cyber bullying or teasing others online? YES
74. Does the child have rules for their online activities inside and outside the home? YES
75. Does the child know what security software friends have at their homes and/or on their mobile devices? YES
76. Does the child know to tell you or a trusted adult if they unintentionally receive pornographic content? YES
77. Does the child have daily time limits for being online? YES
78. Does the child go online at the same time every night? NO
79. Does the child know to tell you or a trusted adult if they receive an online sexual message? YES
80. Does the child only download legal files, music and videos? YES
81. Does the child know to tell you if they are contacted by an adult stranger online? YES
82. Does the child spend less time with friends and more time online? NO
83. Does the child have an online curfew to shut down their computer? YES
84. Would the child talk to you, a teacher or trusted adult if they felt unattractive, unpopular, angry or sad? YES
85. If the child felt angry, sad or depressed, would he or she chat with an online stranger? NO
86. Does the child feel more comfortable online than spending time with friends or family? NO
87. Has the child become less interested in their favorite offline activities? NO
88. Does the child engage in online or offline risk-taking considered self-destructive? NO
89. Has the child fell behind in school due to their online activities? NO
90. Has the child's behavior changed for the worse due to their online activities? NO
91. Does the child feel stressed, anxious or depressed because of conflict at home or school? NO
92. Does the child spend more time online than offline with friends or family? NO
93. Does the child check their social accounts more than twenty times a day? NO
94. Does the child have a social profile with information available to the public? NO
95. Does the child share their private or personal details on a blog or online diary? NO
96. Does the child visit chat rooms without adult or online moderators? NO
97. Does the child have a Twitter account you or loved ones do not check? NO

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)

98. Does the child allow people they do not know join their friends or buddy list to have big lists? NO
99. Does the child often visit and interact with online users in chatrooms that allow sexually explicit discussions or not moderators? NO
100. Does the child visit pornography or sex sites online? NO
101. Has anyone ever posted embarrassing information about the child? NO
102. Is the child cautious when posting personal information online? NO
103. Do you or the child know what digital reputation means? YES
104. Has the child shared confidential information to an ex-friend online? NO
105. Does the child practice caution what they disclose to others online? YES
106. Does the child protect their images and videos from strangers viewing them? YES
107. Do you and the child know and discuss their digital footprint? YES
108. Does the child know their photographs can remain in cyberspace for years? YES
109. Does the child know information shared online may become "viral"? YES
110. Does the child have a mobile device with information that is embarrassing? NO

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

Correct Responses__+ Does Not Apply Responses__= IPI-P 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 often 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 iPredator 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 iPredator 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 iPredator 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 iPredator 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 iPredator 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 iPredator 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 iPredator 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.