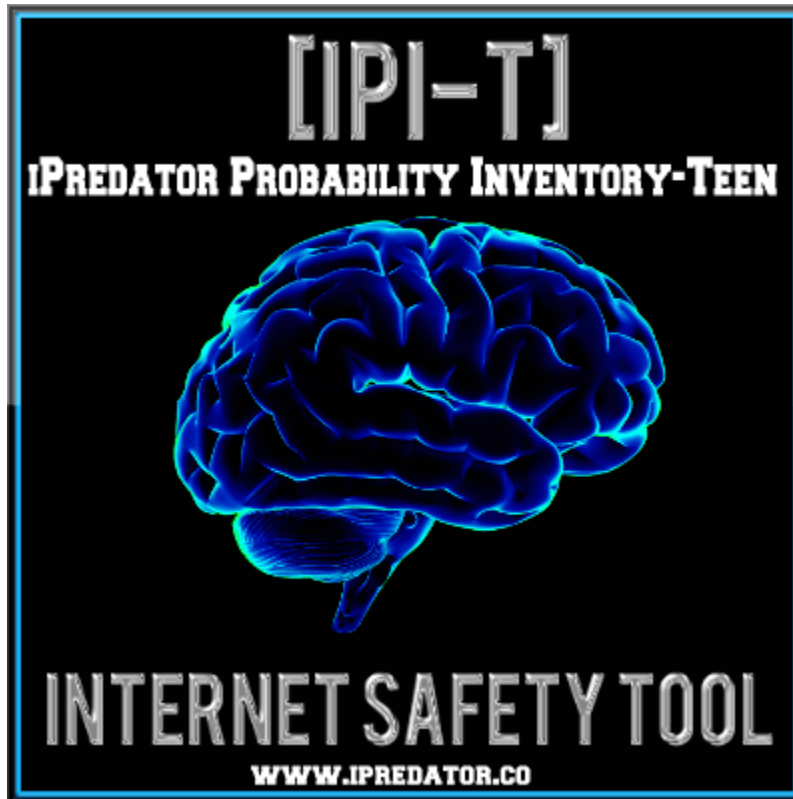


# IPI-T

iPredator Probability Inventory - Teen

Michael Nuccitelli, Psy.D.

[www.ipredator.co](http://www.ipredator.co)



## iPredator Probability Inventory - Teen (IPI-T)

The iPredator Probability Inventory - Teen is a 110-statement diagnostic, education, assessment and data collection tool designed to investigate an adolescent or young adult's online preparedness, vulnerability and risk potential of being targeted by an iPredator. Just as all the IPI assessment collection inventories, the IPI-T focuses on the adolescent's relationship to ICT, their knowledge base of malevolent and nefarious users, environmental aspects influencing their online activities and their practice of the behavioral actions necessary for internet safety and preparedness if cyber attacked.

The IPI-T is completed by 13-18 year-old minors or can be used by adults and educators for educational and data collection purposes. Once completed, the IPI score, ranging from 0-110, represents their preparedness, vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyberstalking, cyber harassment, cyberbullying or trolling for a target to sexually victimize. The IPI-T investigates the areas problematic to all Information Age children and adolescents. Furthermore, the IPI-T also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

## IPI-T DIRECTIONS

1. The time needed to complete the IPI-T 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.



# IPI-T

**Note:** The IPI-T is formatted in the “You” tense to enable an adolescent to take the inventory as the respondent. If an adult or parent is completing the inventory, please replace “You” with “The Teen”.

Gender: Male\_\_ Female\_\_

Age: (11-14) \_\_ (15-16) \_\_ (17-18) \_\_

Average Daily Online Activity: 0-1Hours \_\_ 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. Has anyone been mean to you online and kept it a secret from your parents or a trusted adult? NO
2. Have you harassed or teased someone online and kept it a secret from your parents or a trusted adult? NO
3. Have you been "flamed" online and kept it a secret from your parents or a trusted adult? NO
4. Have you sent, posted or received mean messages about others and did not tell anyone? NO
5. Have you had an online relationship go bad and they began teasing or harassing you online? NO
6. Have you had secrets spread by others online and kept it a secret from your parents or a trusted adult? NO
7. Do you know what to do if you or a friend is being teased, harassed or cyberbullied? YES
8. Are you careful about what you disclose to others online? YES
9. Do you protect your images or videos from strangers viewing them? YES
10. Have you been harassed or teased online on the grounds of your race, religion, gender, sexuality or physical look? NO
11. Have you ever retaliated to online information being spread about you and did not ignore their harassment or teasing? NO
12. Are you careful about posting your personal information online and know why it is so important related to your digital reputation? YES
13. Do you know what "digital footprint" means or how posting your personal information online can hurt your reputation? YES
14. Have you shared confidential information to a now ex-friend online and concerned about what they will do with the information? 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)

15. Do you have a positive "digital reputation" or know how to create a positive "digital reputation?" YES
16. Do you know the images and videos you post online can remain in cyberspace for years? YES
17. Did you know sensitive and sexual information you share online might be impossible to delete? YES
18. Do you know "sexting" involving you or friends can be shared with others without your consent? YES
19. Do you or have you had sexual conversations with someone met online? NO
20. Do you tell your friends or coworkers your passwords? NO
21. Have you called, text messaged or chatted online with strangers? NO
22. Have you ever been contacted by an online stranger and kept it a secret or not told loved ones? NO
23. Have you ever met someone in person you met online and did not tell loved ones? NO
24. Do you respond to adult online strangers who initiate contact? NO
25. Do you communicate with people you do not know online and keep it a secret from loved ones? NO
26. Do you have a mobile device (i.e., cell phone, smart phone) with information on it that is embarrassing, sexual or secret? NO
27. Have you been educated or educated yourself on internet predators, cyber harassment and cybercrime? YES
28. Are you aware iPredators target children, teens and adults using kindness and understanding? YES
29. Do you know how iPredators engage in identity theft and practice online identity protection? YES
30. Do you know iPredators will encourage you and your friends to add them to their "buddy" and "friends" lists? YES
31. Do you give your mobile device or cell phone passwords to loved ones you trust implicitly? YES
32. Do you know how to prevent unwanted access to your mobile devices or cell phone? YES
33. Have you been educated on the dangers of GPS location services? YES
34. Do you know GPS location services allow anyone to know your exact location at any given time? 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)

35. Are you aware iPredators use attention, affection and gifts to seduce children, teens and adults online? YES
36. Do you know iPredators may create online profiles pretending to be someone you think are attractive and intriguing? YES
37. Do you know what peer-to-peer networks are and how they can expose your computer and network to iPredators? YES
38. Do you know most children and adults are victimized by family members, friends and trusted peers? YES
39. Do you know to be suspicious of anyone online who encourages you to be defiant, deceptive or lie to loved ones or coworkers? YES
40. Do you know iPredators look for children, teens and adults who will access their phones or the internet during late night hours? YES
41. Do you spend time learning mobile device and mobile phone safety? YES
42. Do you know how to install security on your mobile devices or mobile phone? YES
43. Do you follow school or work policies regarding mobile device and mobile phone usage? YES
44. Have you downloaded and installed antivirus software on your mobile devices? YES
45. Do you post your home or cell phone numbers on sites available to the public? YES
46. Do you know it is beneficial to have multiple passwords and to change them often? YES
47. Do you visit "private" chat rooms or questionable websites and keep it a secret from loved ones? NO
48. Are you familiar with bot software, spyware, keystroke loggers and viruses? YES
49. Do you know that social media sites are often frequented by iPredators? YES
50. Are you prepared when friends and loved ones introduce you to questionable and high-risk web sites? YES
51. Do you know that you can accidentally show your phone number by Caller ID to others you do not know? YES
52. Do you know what to do if you are exposed to sites dealing with hatred, violence, racism or graphic content you consider inappropriate? YES
53. Do you post your home or cell phone numbers online? NO
54. Do you exchange images or videos with others you have met online and have never met? NO
55. Do you always log off when not using instant messaging or your email accounts? YES
56. Do you know about the dangers of disclosing your personal and/or contact information online? 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)

57. Do any of your user accounts or profile names include your full or partial real name?  
NO
58. Do you post your full name, home phone number or home address online at social or business networking sites? NO
59. Do you refrain from sharing your social security number online? YES
60. Do you click on links in your email from unknown senders? NO
61. Is your school, college or employment website password protected regarding the viewing of student or employee contact information? YES
62. Do you know to never give your credit card information online unless you are 100% sure the payee is trustworthy? YES
63. Do you know how to recognize identity thieves that pretend to be a trusted organization and ask you to verify your personal information? YES
64. Do you send sensitive information such as credit card numbers by email? NO
65. Do you only download legal files, music and videos? YES
66. Do you spend less time with friends or family and more time online? NO
67. Do you have a personal cut-off time for being online if it is not school or work related?  
YES
68. Would you talk to loved ones or a professional if you felt depressed, distressed or angry? YES
69. Do you feel angry, anxious, sad or depressed? NO
70. Do you feel more comfortable online than spending time with your friends, coworkers or family? NO
71. Have you become less interested in your favorite offline activities? NO
72. Has loved ones or coworkers recently said you have changed or isolating more? NO
73. Do you feel stressed or anxious because of what is going on at home, school or work?  
NO
74. Have you been less attentive, less productive or falling behind in school, work or major responsibilities? NO
75. Do you have a Facebook or social media account you access more than 7-10 times a day? NO
76. Do you make sure you set and often check your privacy settings? YES
77. Do you allow others you do not know join your "friends" list? NO
78. Do you limit who can view your photos and videos at your profile page? YES
79. Do you have a social media profile with information available to the public? NO
80. Do you share with others private and personal details at your social media profile? 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)

81. Do you review the privacy and security settings at social media sites you have joined?  
NO
82. Do you restrict your picture at your social media profile for the public to see other than public figure or fan pages? YES
83. In chatrooms, do you use a nickname that is different from your screen name? YES
84. With social media accounts, is your screen name safe for creating an online identity?  
YES
85. If your online identity is different from your real-world identity, do you still practice internet safety? YES
86. Do you set your privacy settings in your profiles as private? YES
87. Do you post inappropriate or sexually provocative images online? NO
88. Do you post inappropriate or sexually provocative comments online? NO
89. Do you post inappropriate or sexually provocative comments in chatrooms? NO
90. Do you respond to inappropriate or sexually provocative comments in chatrooms? NO
91. If you get an angry IM or comment on a message board or blog, do you wait a few minutes and calm down before responding? YES
92. Do you post, share or distribute copyrighted images, songs or files? NO
93. Do you type your screen name or email address into search engines and see what comes up? YES
94. Do you buy things online without talking to your parents or a trusted adult first? NO
95. Do you talk to your parents or a trusted adult first before you open an email attachment or download software? YES
96. Do you talk to your parents or a trusted adult first about safe and accurate websites for research? YES
97. If you are planning to meet somebody you met online, do you or would you bring a friend or trusted adult to the first meeting? YES
98. If you get suspicious e-mails, files or pictures from someone you do not know and trust, do you delete them before opening them up? YES
99. Are you cautious about posting information that could identify or locate you offline? YES
100. Do you flirt with strangers online? NO
101. Do you make sure you set and often check your privacy settings? YES
102. Do you allow others you do not know join your "friends" list? NO
103. Do you limit who can view your photos and videos at your profile page? YES
104. Do you spend large periods online involved with social networking sites? NO
105. Do you have a social media profile with information available to the public? NO

106. Do you share with others private and personal details at your social media profile? NO  
 107. Do you share your email, home address or telephone numbers online without being sure of what you are doing? NO  
 108. Do you review the privacy and security settings at social media sites you have joined? NO  
 109. Do you restrict your picture at your social media profile for the public to see other than public figure or fan pages? YES  
 110. Do you have a genderless screen name? 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)

Yes Answers \_\_ No Answers \_\_ I Do Not Know \_\_ Does Not Apply \_\_

Correct Responses \_\_ + Does Not Apply Responses \_\_ = IPI-T Score \_\_

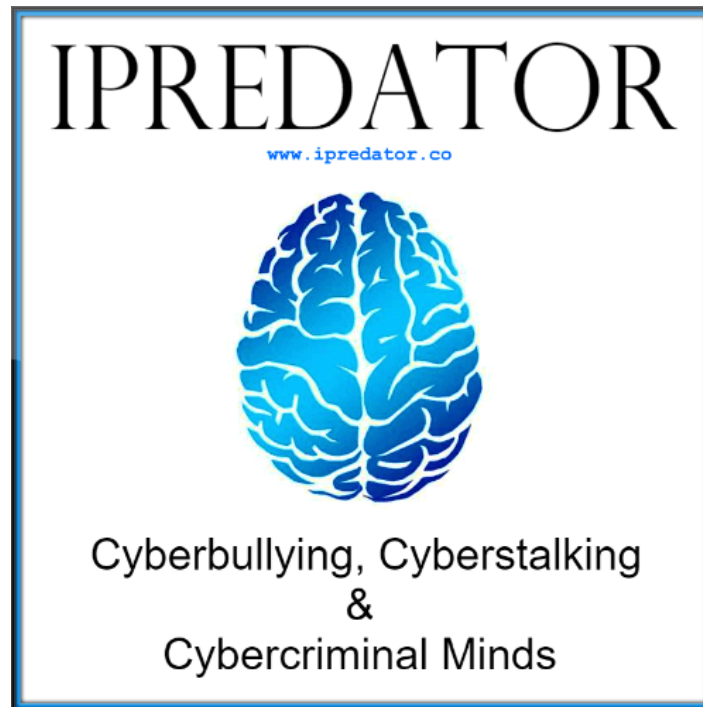


**Note:** The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. “I Do Not Know” & “No” responses should be addressed at once with a plan of action. Although obtaining a score of 90 or higher indicates a minimal probability of a successful cyber-attack, it is still 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.

# IPREDATOR

## IPI SCORING KEY

### **IPI Score: (1-10)**

**Category:** Guaranteed iPredator Target

**Risk Potential:** Alarming 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 parties and the media at no cost. The [iPredator](#) website and everything created by Dr. Nuccitelli is educational, free and public domain.