IPI-330

iPredator Probability Inventory - 330

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

iPredator Probability Inventory - 330 (IPI-330)

The iPredator Probability Inventory- 330 is a 330-question diagnostic, education, assessment and data collection tool designed to investigate a 6-18-year-old minor about their online victimization risk potential, cyber-attack awareness and support system involvement. A parent, educator, family member or pediatric professional completes the IPI-330.

Just as all the IPI assessment collection inventories, the IPI-330 focuses on a child and/or students 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.

Once completed, the respondent tabulates their score, ranging from 0-330 and stands for the child, adolescent or young adult's risk potential and vulnerability of being targeted by an iPredator engaged in cyberbullying, cybercrime, cyberstalking, cyber harassment or trolling for targets to sexually victimize.

As the inventory name states, the IPI-330 is a 330-question inventory segmented into 11 categories relevant to all online users and can be conducted all at once or used in parts focusing on the parent or educator's goals and strategies. The IPI-330 also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-330 DIRECTIONS

1. The time needed to complete the IPI-330 inventory averages 90-120 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 give information. ICT stresses the role of unified communications and the integration of telecommunications, which enable users to create access, store, send 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, name, find, 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-330

Child's Gender: Male__ Female__
Age: (6-12) __ (13-14) __ (15-16) __ (17-18) __
Average Daily Online Activity: 0-1 Hours __ 1-3 Hours __ 3-5 Hours __ 5+ Hours __

Note to Respondent: Anytime the term "online" is used in the inventory, please also keep in mind it applies to all forms of Information and Communications Technology (ICT.) The correct response to each question is "Yes" or "No" after each question.

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)

CYBERBULLYING

1. Do you regularly discuss cyberbullying with the child? YES
2. Has the child returned home with missing or damaged belongings? NO
3. Does the child know how to ignore being harassed or teased online and why it is important? YES
4. Has the child been flamed (a provoking message) online and retaliated? NO
5. Has the child been harassed or teased online about their race or sexual orientation? NO
6. Has the child been threatened, embarrassed or teased online about their physical attributes? NO
7. Has the child been negative about school or their home environment stemming from their online activities? NO
8. Has anyone sent or posted harmful messages about the child online? NO
9. Has the child been teased or embarrassed by someone online that you or trusted adult do not know? NO
10. Has the child had an online relationship involving a negative outcome cause them distress? NO
11. Has the child had secrets spread by others online without their consent? NO
12. Has anyone captured, saved or stored embarrassing information about the child? NO
13. Has the child retaliated to online information being spread about them? NO
14. Has the child been repeatedly harassed or berated by someone online? NO
15. Does the child know how to respond if a friend is being cyberbullied? YES
16. Does the child know about cyberbully bystander? YES
17. Has the child received offensive online information and became anxious? NO
18. Has the child been sexually teased or taunted online? NO
19. Has the child been aggressive and/or mean to others online? NO
20. Would the child be a bystander if their friend was being teased online? NO
21. Does the child know what encourages a cyberbully? YES

22. Does the child appear sullen going to or returning from school connected to their online activities? NO
23. Does the child know content they share online can be used to embarrass them? YES
24. Does the child practice good "*Digital Citizenship*". YES
25. Does the child know what to do if they are being taunted by others? YES
26. Has the child received offensive information sent to their mobile devices? NO
27. In the last 90 days, has anyone repeatedly teased the child online? NO
28. In the last 90 days, has anyone repeatedly lied to the child online? NO
29. In the last 90 days, has the child been bullied offline? NO
30. In the last 90 days, has anyone shared embarrassing content about the child online? 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)

DIGITAL REPUTATION

31. Has anyone posted truthful, but embarrassing information about the child online? NO
32. Is the child cautious when posting personal and sensitive information online? YES
33. Does the child know what "*Digital Footprint*" means? YES
34. Has the child shared confidential information to a now ex-friend or ex-intimate partner they first met online? NO
35. Does the child practice caution and restraint what they share online? YES
36. Does the child protect their photographs, images and videos from online strangers viewing them? YES
37. Does the child have a positive "*Digital Reputation*"? YES
38. Does the child know their content can remain in cyberspace for years? YES
39. Does the child know information shared online may be impossible to remove? YES
40. Does the child have a mobile device with information that is embarrassing or sexual in nature? NO
41. Does the child know "*Sexting*" can be criminal if the subject is a minor and shared with others if they are the subject? YES
42. Does the child know their personal information they post online can go viral? YES
43. Does the child know how to establish and maintain a positive *"Digital Footprint"*? YES
44. Does the child know images and videos can be reposted multiple times? YES
45. Does the child know what information can be harmful to their online reputation? YES
46. Do you ensure the child's digital reputation is correct? YES
47. Do you check what information the child disseminates online? YES
48. Does the child practice good behavior online and in chat rooms? YES
49. Do you enter the child's personal information into search engines? YES
50. Do you check the child's email and social media profiles? YES
51. Has the child engaged in sexting? NO
52. Do you spend time with the child educating them on their digital reputation? YES
53. Does the child know the content they share online can be reposted? YES

54. Does the child understand how information shared online can harm their prospects? YES
55. Does the child share provocative photos, videos or details online? NO
56. Does the child post personal information online to impress others? NO
57. Has the child shared confidential information to an ex-friend or ex-partner they wish they could retract? NO
58. Is the child careful what they show to others using their mobile devices? YES
59. Does the child refrain from sharing images and videos with online strangers? YES
60. Does the child know offensive information shared online is impossible to remove? YES
61. Has the child had sexual conversations with someone they met online? 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)

HIGH RISK BEHAVIORS

62. Did the child have a social media account prior to age 13? NO
63. Does the child refuse to show websites they have visited? NO
64. Has the child visited or been exposed to online sex sites? NO
65. Does the child often use the internet without supervision? NO
66. Has the child received or made phone calls to others you do not know? NO
67. Does the child inform others online when an adult will not be home? NO
68. Has the child been contacted by the same online stranger more than once? NO
69. Has the child ever met someone in person he or she met online? NO
70. Has anyone approached the child unexpectedly and the child quickly shut off his or her device? NO
71. Does the child know why responding to online strangers can be dangerous? YES
72. Has the child been contacted by an adult online recently introduced to them by an online peer? NO
73. Does the child communicate online with adults you do not know? NO
74. Does the child isolate in his or her room while online for reasons other than productive? NO
75. Does the child visit chat rooms without an adult's permission? NO
76. Does the child use a computer or mobile device in their room with the door closed? NO
77. Has the child engaged in online activities they have been restricted from? NO
78. Does the child know to log out if they feel uncomfortable by online contacts? YES
79. Does the child engage in online activities they do not want you to know about? NO
80. Would the child meet someone they met online without your permission? NO
81. Does the child know they are at a higher risk being contacted by online strangers at night? YES
82. Has the child ever planned to meet someone they have met online without your knowledge? NO
83. Does the child accept free software from online strangers? NO

84. Does the child hesitate to show you who they converse with online? NO
85. Does the child have "buddy" or "*friend*" lists with online users you do not know? NO
86. Does the child share their sexual orientation to online strangers? NO
87. Has the child discussed sexually themed topics in chat rooms with online users they do not know? NO
88. Has the child text messaged, tweeted or chatted about sex online with others? NO
89. Has the child been contacted by an online stranger seeking their home address? NO
90. Has the child met someone in person he or she met online without a friend or family member? 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)

IPREDATOR AWARENESS

91. Are you confident the child has been educated on iPredators? YES
92. Are you aware iPredators target children using kindness and understanding? YES
93. Are you aware iPredators use attention, affection and gifts to seduce children? YES
94. Are you aware most iPredators are the same age as the child? YES
95. Does the child know iPredators create profiles pretending to be their same age? YES
96. Are you aware iPredators are educated in areas that intrigue children? YES
97. Do you know the ideal age an iPredator targets is between 11 and 14? YES
98. Does the child know iPredators encourage others to add them to their "*buddy*" lists? YES
99. Do you know peer-to-peer networks can expose your child's computer to iPredators? YES
100. Do you know the best protection from iPredators is effective online communication? YES
101. Do you know how to block sites on your child's devices from being accessed by iPredators? YES
102. Do you know iPredators use keywords at their sites popular to children? YES
103. Are you aware many children, aged 8-12, explore sex sites? YES
104. Does the child know adults will pretend to be minors with fake profiles? YES
105. Have you been taught about online predators and the "*Grooming*" process? YES
106. Is the child suspicious of anyone online who encourages them to be defiant to authority? YES
107. Do you know iPredators encourage children to keep their contacts secret? YES
108. Are you aware most iPredators will be encouraging, patient and reserved? YES
109. Are you aware iPredators offer children their online accounts to converse? YES
110. Are you aware iPredators will embed popular child search terms in their websites and usernames? YES
111. Are you aware iPredators consistently tell children they are always available if needed? YES
112. Are you confident the child does not use fake online identities? YES

113. Are you educated on "*Grooming*" by iPredators in their quest to exploit children? YES
114. Do you know file-sharing sites allow iPredators to access portions of your child's computer? YES
115. Does the child know iPredators encourage children to share their images, videos or appear on webcam? YES
116. Does the child know iPredators encourage children to share privileged information without being overbearing? YES
117. Does the child know most iPredators act kind and understanding online? YES
118. Does the child know iPredators offer gifts to minors they are targeting? YES
119. Does the child know iPredators will try to steal their identity? YES
120. Does the child know iPredators create profiles pretending to be their age with similar interests? 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)

MOBILE DEVICE TECHNOLOGY

121. Do you restrict the child from their mobile devices during late night hours? YES
122. Do you know children must be 18 years old to activate their GPS services? YES
123. Does the child's mobile devices have unlimited text messaging and online access? NO
124. Do you know the passwords to the child's mobile devices? YES
125. Do you know how to prevent unwanted access to the child's mobile devices? YES
126. Do you track the images and video sent from the child's mobile devices? YES
127. If you have a home WiFi system, do they run added firewalls? YES
128. Have you educated the child on the dangers of GPS location services? YES
129. Do you know GPS location services allows anyone to know the child's exact location? YES
130. Have you contacted mobile device services about security controls for the child? YES
131. Do you spend time learning mobile device safety? YES
132. Do you know how to install security on the child's mobile devices? YES
133. Do you know about "*Near Field Communications*" and mobile devices to make purchases? YES
134. Do you know children favor text messaging as their primary means of communicating with peers? YES
135. Do you know how to set up remote lock and wipe features in mobile devices? YES
136. Do you know how to install security software on the child's mobile devices? YES
137. Do you check the stored images and video on the child's mobile devices? YES
138. Have you installed antivirus software on the child's mobile devices? YES
139. Does the child know to treat their mobile devices as carefully as their wallets? YES

140. Do you discourage the child from sharing confidential information with their mobile devices? YES
141. Does the child silence their mobile devices in public places? YES
142. Do you set age-appropriate restrictions on the child's mobile device usage? YES
143. Does the child follow school policies about mobile device usage? YES
144. Are you aware there are few methods of filtering web content on mobile devices? YES
145. Are you aware that pornographic content is more accessible on mobile devices? YES
146. Are you aware a trend for children is "*Sexting*" using their mobile devices? YES
147. Does the child give their mobile phone passwords to you? YES
148. Does the child know how to prevent access to their mobile phone? YES
149. Has the child learned about the dangers of GPS location services? YES
150. Does the child know GPS location services allow anyone to know their exact location? 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)

ICT AWARENESS

151. Are you aware the child will be introduced by peers to questionable websites? YES
152. Does the child know to never share his or her password with close friends? YES
153. Do you know there is no filtering software that can replace adult supervision? YES
154. Do you know the child may accidentally show his or her phone number by "*Caller ID*"? YES
155. Do you know it is beneficial for the child to have multiple passwords? YES
156. Are you aware the child has access to their friends' computers and mobile devices? YES
157. Do you discourage the child from entering private chat rooms? YES
158. Are you aware the child may be exposed to sites dealing with hatred? YES
159. Do you discourage the child from activating their geolocation services? YES
160. Are you familiar with bot software, spyware, keystroke loggers and viruses? YES
161. Do you know that online gaming systems provide extensive communication features? YES
162. Are you prepared for the child visiting adult content websites? YES
163. Are you aware there is technology to identify people the child interacts with if needed? YES
164. Do you know how to set the child's computer security settings on high? YES
165. Are you familiar with home wireless networks (WiFi) and their security settings? YES
166. Does the child participate in online activities you do not approve of? YES
167. Do you know what to do if your child is targeted by identity thieves? YES
168. Does the child know to never click a link in an unknown email or instant message? YES
169. Can you define unintentional vs. intentional access to offensive web content? YES

170. Does the child know not to click on the links in the video comments section? YES
171. Are you aware websites use keywords from the top twenty brand names for children? YES
172. Do you have filters and security software installed to make chatrooms inaccessible? YES
173. Do you know how to disable the preview function in the child's email? YES
174. Do you know parental control software helps limit the sites the child can access? YES
175. Have you installed security controls on the child's mobile devices? YES
176. Do you know adult pornography websites format their sites, so children will inadvertently visit them? YES
177. Do you know there is no filtering software that can completely insulate a child from iPredators? YES
178. Are you aware the child has access to their friends' computers and mobile devices when adult supervision is absent? YES
179. Do you know that online gaming systems provide extensive communication features allowing online strangers to contact them? YES
180. Do you know how to confirm the child's privacy settings are set on "friends only"? 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)

PERSONAL INFORMATION

181. Does the child post their home or cell phone numbers on sites without your permission? NO
182. Does the child know to be cautious sharing their contact information on gaming sites? YES
183. Does the child know not to exchange images or video with someone they met online? YES
184. Does the child always log off when not using instant messaging? YES
185. Do you educate the child about the dangers of disclosing personal information? YES
186. Are you confident the school's website is password protected? YES
187. Is the child cautious posting their email address to prevent "*Screenscrapers*"? YES
188. Does the child post their school's name online without your permission? NO
189. Do you educate the child about the dangers of sharing personal information online? YES
190. Do you encourage the child to be cautious sharing personal information? YES
191. Do the child's online usernames include their full or partial real name? NO
192. Does the child post their full name or address without a teacher or your knowledge? NO
193. Does the child know how to hide displaying their ID or personal information? YES
194. Does the child post their email address on sites without your permission? NO

195. Does the child use text messaging to communicate with others you do not know? NO
196. Does the child regularly disclose their contact information to online contacts? NO
197. Does the child post images in replacement of their own images? YES
198. Is the child consistently posting their full name, home address or telephone number on social sites? NO
199. Does the child use various email addresses for different purposes? YES
200. Do the child's email accounts have the highest level of spam filtering activated? YES
201. Does the child post their home address on social sites without your permission? NO
202. Does the child post their image on social sites without your permission? NO
203. Does the child post their personal information on social sites without concern or caution? NO
204. Do you educate the child about sharing their contact information? YES
205. Does the child include their contact information in their social site profiles or comments? NO
206. Do you monitor who the child allows to have their contact information? YES
207. Does the child know how showing their personal information can lead to online stranger contacts? YES
208. Has the child shared classified information involving parental finances such as credit card information? NO
209. Is the child careful what they disclose to online contacts even when known by family members? YES
210. Does the child protect their images and video from online strangers viewing them on social sites? 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)

IPREDATOR PROTECTION

211. Do you know how to check the child’s internet history? YES
212. Does the child know to consult a trusted adult if exposed to graphic content? YES
213. Do you discourage the child from being a party to cyberbullying? YES
214. Do you know how to deactivate the child’s “*Caller ID*” services? YES
215. Do you know to contact the police if the child is sexually solicited online? YES
216. Do you encourage a teacher or trusted adult to set rules for the child's online activity inside and outside the home? YES
217. Are you familiar with common chat room lingo used by children? YES
218. Do you know what computer safeguards the child's friends have in their homes? YES
219. Are the child's instant messaging contacts and “*buddy*” lists discussed regularly? YES
220. Do you monitor pornographic content on the child’s computer? YES
221. Does the child have daily time limits for being online? YES
222. Have you blocked access from the child visiting adult content websites? YES

223. Do you prohibit the child from online activity during late night hours unless supervised and productive? YES
224. Do you monitor the child's friend lists on their social sites? YES
225. Do you engage the child in discussions about their friend's online habits? YES
226. Do you encourage the child to tell an adult if they receive an online sexual solicitation? YES
227. Do you remind the child to only download legal files, music and videos? YES
228. Do you know how to respond if the child explores sexual websites? YES
229. Do you have a plan if the child is contacted by someone suspicious online? YES
230. Do the adults supervising the child when visiting friends have online rules? YES
231. Do you discuss with the child possible online dangerous scenarios? YES
232. Do you know how to check the child's history folder if you become suspicious? YES
233. Do you confirm chatrooms are always monitored by a trained moderator? YES
234. Do you limit the child's online chatting on their favorite gaming or club sites? YES
235. Does the child know you visit the websites they frequent? YES
236. Do you keep all ICT in a public area of your home that is central to your view? YES
237. Do you know to contact the police if the child reports being sexually solicited online? YES
238. Do you set rules inside and outside the home for the child's online activities? YES
239. Are the child's instant messaging contacts and "*buddy*" lists checked regularly? YES
240. Do you monitor the child's friend lists and encourage adult confirmation first? 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)

PSYCHOLOGICAL STATES

241. Does the child spend less time with friends and more time online? NO
242. Does the child have an online curfew? YES
243. Does the child report he or she feels unattractive or not liked? NO
244. Does the child exhibit appear sad or depressed causing an increase in online activities? NO
245. Does the child post comments not typical of their age online? NO
246. Has the child withdrawn from his or her favorite activities by spending more time online? NO
247. Does the child engage in risk-taking and/or self-destructive behaviors connected to their online activities? NO
248. Has the child had a drastic change in grades related to their online activities? NO
249. Has the child been less attentive or falling behind in school related to their online activities? NO
250. Has the child's behavior changed without explanation somehow related to their online activities? NO
251. Does the child seem distressed or anxious related to their online activities? NO

252. Does the child have little adult involvement or none? NO
253. Has the child reported a loss of appetite or lack of sleep related to their online activities? NO
254. Has the child withdrawn from friends and family members due to their online activities? NO
255. Does the child prefer online contacts to offline friends? NO
256. Does the child complain about stomachaches or feeling ill suspected of being related to their online activities? NO
257. Do you define the child as being defiant and/or oppositional related to their online activities? NO
258. Has the child witnessed a traumatic event or adult conflict, which led to an increase in their online activities? NO
259. Does the child report disliking school, the teachers or other children related to their online activities? NO
260. Has the child reported not feeling accepted by his/her peers related to their online activities? NO
261. Does the child report feeling more accepted by adults due to their online activities? NO
262. Does the child appear hopeless and/or discouraged due to their online activities? NO
263. Does the child become easily upset related to their online activities? NO
264. Does the child spend more time online and/or uninterested in family functions? NO
265. Does the child become easily agitated and/or externalizes blame related to their online activities? NO
266. Do the child's friends have behavioral/emotional problems in school related to their online activities? NO
267. Has the child had a drastic change in grades due to his or her online activities? NO
268. Does the child have little adult involvement due to his or her online activities? NO
269. Has the child reported a loss of appetite or lack of sleep due to their online activities? NO
270. Does the child complain about feeling overwhelmed or distressed due to his or her online activities? 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)

SOCIAL MEDIA

271. Does the child spend large periods online involved with social media? NO
272. Does the child know to end online contact if someone initiates questions about sex? YES
273. Does the child have a social account you rarely access? NO
274. Does the child have a social media profile with information available to the public? NO
275. Does the child often share with others his/her social media profile? NO

276. Do you know the age restrictions of the child's favorite social media sites? YES
277. Does the child visit chatrooms without adult moderation? NO
278. Does the child know to be cautious of flattering messages received online from unknown contacts? YES
279. Does the child keep their profile pages private only for invited friends? YES
280. Do you spend time educating the child on proper online etiquette? YES
281. Do you monitor social media sites the child frequents? YES
282. Do you join and become a "*friend*" or "*buddy*" on the child's social profiles? YES
283. Does the child have a mobile device with an application to their social media profile they habitually use? NO
284. Does the child limit who can view photos and videos on their social profile page? YES
285. Are you aware most social sites require a child to be 13 years old before they can sign up? YES
286. Do you review the privacy and security settings on social media sites with the child? YES
287. Does the child know social media, when used carelessly, is dangerous? YES
288. Do you prohibit the child from posting their picture in a public profile? YES
289. Does the child have a social account you do not monitor? NO
290. Does the child allow people they do not know join their "*friends*" list? NO
291. Does the child have their privacy settings set to "*Friends of Friends*" or "*Public*"? NO
292. Does the child refuse friend requests from others they do not know? YES
293. Does the child refrain from responding to strange messages? YES
294. Is the child respectful online and shares positive information when prompted? YES
295. Is the child aware people they meet online may lie about who they are and their interests? YES
296. Does the child practice caution with their social profiles? YES
297. Does the child know to end contact if someone starts with questions leading to their home location? YES
298. Does the child know to be cautious of flattering messages from others they meet online? YES
299. Do you spend time educating the child on proper online etiquette? YES
300. Do you join and become a "*friend*" or "*buddy*" on the child's social site profiles? 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)

CYBERSTALKING

301. Does the child give out their Social Security Number to unknown online requests? NO
302. Does the child know what to do if they receive harassing or unwanted communications? YES
303. Does the child know cyberstalkers pose as their victim and attack others online? YES

304. Does the child know what to do if receiving unwanted emails or text messages from an ex-partner, acquaintance or stranger? YES
305. Does the child know what to do if receiving unsolicited threatening emails and/or death threats? YES
306. Does the child know what to do if receiving electronic viruses from an ex-partner, acquaintance or stranger? YES
307. Does the child know what to do if receiving spam from an ex-partner, acquaintance or stranger? YES
308. Does the child know what to do if sexually harassed via online posts, emails and phone or text messages? YES
309. Does the child know what to do in chatrooms if cyber harassed, slandered or cyberbullied? YES
310. Does the child know what to do if they find their personal or financial information online posted by an ex-partner, acquaintance or stranger? YES
311. Does the child know what to do if subscribed to pornography and/or distasteful advertising without their consent? YES
312. Does the child regularly check their computers, cell phones and mobile devices for spyware? YES
313. Does the child check their mobile devices if they are being tracked by GPS technology? YES
314. Does the child check if their phone calls or messages are being intercepted? YES
315. Does the child know what to do if being impersonated online? YES
316. Does the child know if being cyberstalked, slandered or harassed, there is a good chance it is an ex-partner, acquaintance or peer? YES
317. Does the child know cyberstalkers contact the victim or the target's family, employer, school and financial institution? YES
318. Does the child know posting personal information when blogging have higher rates of cyberstalking and harassment? YES
319. Does the child know cyberstalkers and harassers follow their target from site to site? YES
320. Does the child make sure their email addresses, instant messaging usernames and links cannot be connected to their home location? YES
321. Does the child know online users are particularly susceptible to cyberstalking, slander and harassment if video blogging (vlogging)? YES
322. Does the child know a cyberstalker can be an obsessed love interest or someone with a grudge due to a minor or imagined reason? YES
323. Does the child know cyberstalkers inconspicuously pose as friends, asking innocuous questions used to recover their target's passwords? YES
324. Does the child know that most cyberstalking involves someone they have interacted with in the recent past? YES
325. Does the child know that cyberstalking can occur whether the offender or target lives or works close to their location? YES
326. Does the child know a cyberstalker can be an egotistic aggressor who wants to show-off to their peers, online peers and/or colleagues? YES

327. Does the child know to avoid announcing their physical location via status updates of GPS-enabled applications? YES
328. Does the child know changing Internet Service Providers and reporting hostile and/or aggressive events are recommended to stop cyberstalking? YES
329. Does the child know how to recognize if they are being groomed by and iPredator? YES
330. Does the child know to never leave a logged in computer unattended? YES

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

Correct Responses__+ Does Not Apply Responses__= IPI-330 Score__

Note: The goal for optimal internet safety & cyber security functioning is to score a 300 or higher. *"I Do Not Know"* & *"No"* responses should be addressed immediately with a plan of action. Although obtaining a score of 300 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.

IPREDATOR

IPI SCORING KEY

IPI Score: (0-32)
Category: Guaranteed iPredator Target and Extremely Vulnerable.
Risk Potential: Alarmingly High.
iPredator Involvement: Certain.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Urgent Attention Required.

IPI Score: (33-65)
Category: Prime iPredator Target and Extremely Vulnerable.
Risk Potential: High.
iPredator Involvement: Almost Certain.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Immediate Attention Required.

IPI Score: (66-99)
Category: Probable iPredator Target and Extremely Vulnerable.
Risk Potential: Moderately High.
iPredator Involvement: Involvement Likely.
Intervention Plan: Professional Consultation Highly Advised.
Level of Urgency: Immediate Attention Strongly Recommended.

IPI Score: (100-174)
Category: Likely iPredator Target and Moderate Vulnerability.
Risk Potential: Moderate.
iPredator Involvement: Involvement Suspected.
Intervention Plan: Create and Implement an iPredator Prevention Plan.
Level of Urgency: Immediate Attention Recommended.

IPI Score: (175-249)
Category: Possible iPredator Target and Moderate Vulnerability.
Risk Potential: Moderate.
iPredator Involvement: Involvement Possible.
Intervention Plan: Increase iPredator Protection & Prevention Strategies.
Level of Urgency: Immediate Attention Suggested.

IPI Score: (250-299)
Category: Skilled iPredator Protection.
Risk Potential: Mild.
Predator Involvement: Possible, but Unlikely.
Intervention Plan: Continue iPredator Protection & Prevention Strategies.
Level of Urgency: Not Urgent, Important to Address Below 300.

IPI Score: (300-330)
Category: Advanced iPredator Protection.
Risk Potential: Minimal.
Predator 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.