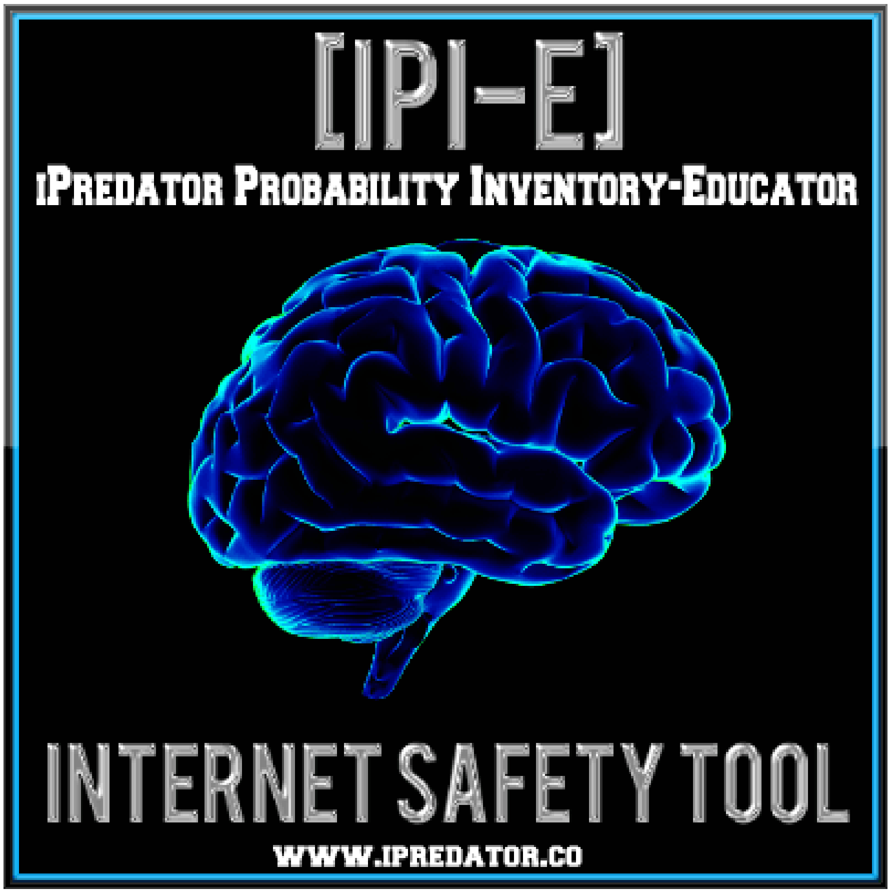
IPI-E

iPredator Probability Inventory - Educator

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



iPredator Probability Inventory - Educator (IPI-E)

The iPredator Probability Inventory - Educator is a 330-question data collection, diagnostic and informational tool for educators regarding a student's online risk potential and vulnerability of being targeted, cyberbullied, cyberstalked, sexually solicited and/or victimized by iPredators. In addition to a data collection tool and general screening exam, the IPI-E can also be used as an adjunct to classroom projects, prevention education plans and educator training seminars on Internet safety. The IPI-E is designed for educators and educational institutions working with children, adolescents and young adults ages 9-21.

Upon completion of the IPI-E, the IPI score ranges from 0-330 and represents the preparedness, probability and risk potential of the student being a targeted by an iPredator engaged in cyberbullying, cybercrime, cyberstalking, cyber harassment or trolling for targets to sexually victimize. The IPI-E 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 educators' goals. The IPI-E also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-E DIRECTIONS

1. The time required to complete the IPI-E inventory averages 90-120 minutes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IPI-e
iPredator Probability
Inventory-Educator
WWW.IPREDATOR.CO

IPI-E

Gender: Male___ Female___
Age: (11-14) __ (15-16) __ (17-18) __ (19-21) __
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)

CYBERBULLYING

1. Do you, a parent or a trusted adult regularly discuss cyberbullying with the student?
YES
2. Has the student returned home with missing or damaged belongings?
NO
3. Does the student know to ignore being harassed or teased online?
YES
4. Has the student been flamed (a provoking message) online?
NO
5. Has the student been harassed or teased about their race or sexual orientation?
NO
6. Has the student been threatened, embarrassed or teased online about their physical attributes?
NO
Has the student been negative about school and/or their home environment?
NO
8. Has anyone sent or posted mean messages about the student online?
NO
9. Has the student been teased or embarrassed by someone you, a parent or trusted adult does not know?
NO
10. Has the student had an online relationship involving adversarial or negative outcomes?
NO
11. Has the student had secrets they have disclosed been spread by others online?
NO
Has anyone captured, saved or stored embarrassing online information about the student?
NO
13. Has the student retaliated to online information being spread about them?
NO
14. Has the student been repeatedly harassed or berated by someone online?
NO
15. Does the student know how to respond if a friend is being cyberbullied?
YES

16. Does the student know who, when and how to report a cyberbully?
YES
17. Has the student received unwanted offensive online content?
NO
18. Has the student been sexually teased or taunted online?
NO
19. Has the student been aggressive and/or mean to others online?
NO
20. Would the student be a bystander if their friend was being harassed and teased?
NO
21. Does the student know what encourages a cyberbully?
YES
22. Does the student appear sullen going to or returning from school due to their online activities?
NO
23. Does the student know pictures they post or share online can be used to embarrass them?
YES
24. Does the student practice good digital citizenship (online manners?)
YES
25. Does the student know what to do if they are being taunted by others online?
YES
26. Has the student received questionable information or images online?
NO
27. In the last 90 days, has someone repeatedly teased the student online?
NO
28. In the last 90 days, has someone repeatedly lie to the student online?
NO
29. In the last 90 days, has the student been cyberbullied?
NO
30. In the last 90 days, has someone repeatedly harass them 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 ever posted embarrassing information about the student online?
NO
32. Is the student cautious when posting personal information online?
YES
33. Does the student know what "digital footprint" means?
YES

34. Has the student shared confidential information to a now ex-friend or ex-intimate partner online?
NO
35. Does the student practice caution what they disclose online?
YES
36. Does the student protect their photographs from strangers viewing them?
YES
37. Does the student have a positive digital reputation?
YES
38. Does the student know their photographs can remain in cyberspace for years?
YES
39. Does the student know information shared online may be impossible to delete?
YES
40. Does the student have a mobile device with information that is embarrassing?
NO
41. Does the student know sexting can be criminal and shared with others?
YES
42. Does the student know their personal information can go viral?
YES
43. Does the student know everyone has an online digital footprint?
YES
44. Does the student know images and videos can be reposted multiple times?
YES
45. Does the student know what information can be harmful to their reputation?
YES
46. Do you, a parent or a trusted adult take steps to ensure the student's digital reputation is accurate?
YES
47. Do you, a parent or a trusted adult respectfully monitor what information the student posts?
YES
48. Does the student practice good behavior online and in chatrooms?
YES
49. Do you, a parent or a trusted adult enter the student's personal information into search engines?
YES
50. Do you, a parent or a trusted adult respectfully check the student’s email and social media profiles?
YES
51. Has the student engaged in sexting?
NO
52. Do you, a parent or a trusted adult spend time with the student educating them on their digital reputation?
YES

53. Does the student know the content they share online can be reposted?
YES
54. Does the student know information shared online can hurt their future?
YES
55. Does the student share provocative photos or details online?
NO
56. Does the student post personal information to impress others?
NO
57. Has the student shared confidential information to an ex-friend online?
NO
58. Are they careful what they tell others online?
YES
59. Does the student know their images and videos can stay in cyberspace for years?
YES
60. Does the student know information they share online may be impossible to delete?
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)

HIGH RISK FACTORS

61. Has the student had sexual conversations with someone they met online?
NO
62. Did the student have a Facebook account prior to age 13?
NO
63. Does the student refuse to disclose websites they have visited?
NO
64. Has the student visited or been exposed to online sex sites?
NO
65. Does the student frequently use the internet without supervision?
NO
66. Has the student received or made phone calls to online strangers you, a parent or trusted adult do not know?
NO
67. Does the student inform others when an adult will not be home online?
NO
68. Has the student ever been contacted by an online stranger?
NO
69. Has the student ever met someone in person he or she met online?
NO
70. Has anyone unexpectedly approached the student and the student shut off his or her computer quickly?
NO

71. Does the student know to avoid responding to unknown adults online?
YES
72. Has the student been contacted by an adult online recently introduced to them?
NO
73. Does the student communicate online with adults a parent or trusted adults do not know?
NO
74. Does the student isolate in his or her room while online?
NO
75. Does the student visit chat rooms without an adult's permission?
NO
76. Does the student use a computer or engage in online activity in their room?
NO
77. Has the student engaged in online activities they have been restricted from by a parent?
NO
78. Does the student know to log out if they feel uncomfortable or fearful?
YES
79. Does the student engage in online activities they do not want a parent or you to know about?
NO
80. Would the student meet someone they met online without parents or your permission?
NO
81. Does the student know they are at a higher risk being contacted by online strangers at night?
YES
82. Has the student met someone they have met online without a parent or your knowledge?
NO
83. Does the student accept free software, ring tones or screen savers from online strangers?
NO
84. Does the student hesitate to disclose whom they converse with online?
NO
85. Does the student have names on his or her “buddy” or “friends” lists unknown to a parent?
NO
86. Does the student send personal information to others online they do not know?
NO
87. Has the student discussed sex online with people they do not know?
NO
88. Has the student text messaged or chatted about sex online with others?
NO
89. Has the student ever been contacted by an online stranger?
NO

90. Has the student ever met someone in person met online without telling a parent or you?
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, a parent or trusted adult confident the student has been educated on iPredators?
YES
92. Are you, a parent or trusted adult aware the iPredator targets children using kindness and understanding?
YES
93. Are you, a parent or trusted adult aware iPredators use attention, affection and gifts to seduce children?
YES
94. Are you, a parent or trusted adult aware most iPredators are roughly the same age as the student?
YES
95. Does the student know iPredators create profiles pretending to be their same age?
YES
96. Are you, a parent or trusted adult aware iPredators are educated in areas that children find intriguing?
YES
97. Do you, a parent or a trusted adult know the ideal age an iPredator targets is between 11-14 years old?
YES
98. Does the student know iPredators encourage others to add them to their “buddy” or “friends” lists?
YES
99. Do you know peer-to-peer networks can expose the student’s computer to iPredators?
YES
100. Do you, a parent or a trusted adult know the best protection from iPredators is effective online communication?
YES
101. Do you, a parent or a trusted adult know how to block sites on computers from being accessed by iPredators?
YES
102. Do you, a parent or a trusted adult know iPredators use keywords at their sites popular to children?
YES
103. Are you, a parent or trusted adult aware many children, aged 8-12, explore sex sites?
YES

104. Does the student know online adult strangers will pretend to be children and teens with fake profiles?
YES
105. Has the student been educated on the "grooming" process used by online sexual predators?
YES
106. Is the student suspicious of anyone who encourages them to be defiant to authority online?
YES
107. Do you, a parent or a trusted adult know iPredators encourage children to keep their contacts secret?
YES
108. Are you, a parent or trusted adult aware most iPredators will be encouraging, patient and reserved?
YES
109. Are you, a parent or trusted adult aware iPredators give children their online accounts to converse?
YES
110. Are you, a parent or trusted adult aware iPredators embed popular child search terms in their sites?
YES
111. Are you, a parent or trusted adult aware iPredators consistently tell children they are always available?
YES
112. Are you, a parent or trusted adult confident the student does not talk with strangers online?
YES
113. Are you, a parent or trusted adult educated on "grooming" by iPredators in their quest to exploit children?
YES
114. Do you, a parent or a trusted adult know file-sharing sites allow iPredators to access portions of their computer?
YES
115. Does the student know iPredators encourage children to share their images and videos?
YES
116. Does the student know iPredators encourage children to share confidential information?
YES
117. Does the student know iPredators are kind and understanding?
YES
118. Does the student know iPredators offer gifts to online users?
YES
119. Does the student know iPredators will try to steal their identity?
YES

120. Does the student know iPredators create profiles pretending to be the student’s age?
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 encourage a parent or trusted adult to restrict the students' mobile devices from late night activity?
YES
122. Do you, a parent or a trusted adult know children must be 18 years old to activate their GPS services?
YES
123. Does the students' mobile devices have unlimited text messaging and online access?
NO
124. Do you, a parent or a trusted adult know the passwords to the students' mobile devices?
YES
125. Do you, a parent or a trusted adult know how to prevent unwanted access to the students' mobile devices?
YES
126. Does a parent or trusted adult track images that are sent from the student’s mobile devices?
YES
127. If the parent or trusted adult has a home WiFi system, do they run additional firewalls?
YES
128. Do you, a parent or a trusted adult educate the student on the dangers of GPS location services?
YES
129. Do you, a parent or a trusted adult know GPS location services allows anyone to know the student's exact location?
YES
130. Have you encouraged a parent or trusted adult to contact the student's mobile device service about adult controls?
YES
131. Do you, a parent or a trusted adult spend time learning mobile device safety?
YES
132. Do you, a parent or a trusted adult know how to install security on the students' mobile devices?
YES
133. Do you, a parent or a trusted adult know about near field communications and mobile devices to make purchases?
YES

134. Do you, a parent or a trusted adult know children favor text messaging as their primary means of communicating?
YES
135. Do you, a parent or a trusted adult know how to set up remote lock and wipe features in mobile devices?
YES
136. Do you, a parent or a trusted adult know how to install security software on the students' mobile devices?
YES
137. Do you, a parent or a trusted adult regularly monitor the stored images on the student's mobile devices?
YES
138. Have you encouraged a parent or trusted adult to download and install antivirus software on the students' mobile devices?
YES
139. Does the student know to treat their mobile devices as carefully as their wallets?
YES
140. Do you, a parent or a trusted adult discourage the student from sharing confidential information with their mobile devices?
YES
141. Does the student silence their mobile devices in public places?
YES
142. Do you encourage a parent or trusted adult to set age-appropriate restrictions on the student's mobile Internet usage?
YES
143. Does the student know and comply with school policies regarding mobile device usage?
YES
144. Are you, a parent or trusted adult aware there are few methods of filtering web content on mobile devices?
YES
145. Are you, a parent or trusted adult aware that pornographic content is more accessible on mobile devices?
YES
146. Are you, a parent or trusted adult aware a new trend for children is sexting using their mobile devices?
YES
147. Does the student give their mobile phone passwords to a parent or trusted adult?
YES
148. Does the student know how to prevent access to their mobile phone?
YES
149. Has the student learned about the dangers of GPS location services?
YES

150. Does the student 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, a parent or trusted adult aware the student will be introduced by peers to questionable websites?
YES
152. Does the student know to never share his or her password with close friends?
YES
153. Do you, a parent or a trusted adult know there is no filtering software that can replace adult supervision?
YES
154. Do you, a parent or a trusted adult know the student may accidentally disclose his or her phone number by Caller ID?
YES
155. Do you, a parent or a trusted adult know it is beneficial for the student to have multiple passwords?
YES
156. Are you, a parent or trusted adult aware the student has access to their friends' computers and mobile devices?
YES
157. Do you, a parent or a trusted adult discourage the student from entering private chat rooms?
YES
158. Are you, a parent or trusted adult aware the student may be exposed to sites dealing with hatred?
YES
159. Do you, a parent or a trusted adult discourage the student from activating their geolocation services?
YES
160. Are you, a parent or trusted adult familiar with bot software, spyware, keystroke loggers and viruses?
YES
161. Do you, a parent or a trusted adult know that online gaming systems provide extensive communication features?
YES
162. Are you, a parent or trusted adult prepared for the student visiting adult content websites?
YES

163. Are you, a parent or trusted adult aware there is technology to identify people the student interacts with online?
YES
164. Do you, a parent or a trusted adult know how to set their computer's security settings on high?
YES
165. Are you, a parent or trusted adult familiar with home wireless networks (WiFi) and their security settings?
YES
166. Does the student participate in online activities a parent or you do not approve of?
YES
167. Do you, a parent or a trusted adult know Facebook is the fastest growing site driven by tweens and teens?
YES
168. Does the student 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 student know not to click on the links in the video comments section?
YES
171. Are you, a parent or trusted adult aware web sites use keywords from the top twenty brand names for children?
YES
172. Do you encourage parents or trusted adults to have filters and security software installed to make chatrooms inaccessible?
YES
173. Do you, a parent or a trusted adult know how to disable the preview function in the student's email?
YES
174. Do you, a parent or a trusted adult know parental control software helps limit the sites the student can access?
YES
175. Has a parent or a trusted adult installed the appropriate security controls on the students' mobile devices?
YES
176. Are you, a parent or trusted adult aware adult websites format their sites, so children will view it?
YES
177. Do you, a parent or a trusted adult know there is no filtering software that can replace adult supervision?
YES
178. Are you, a parent or trusted adult aware the student has access to their friends' computers and mobile devices?
YES

179. Do you, a parent or a trusted adult know that online gaming systems provide extensive communication features?
YES
180. Does a parent or a trusted adult know how to set the student's computer security settings on high?
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 student post their home or cell phone numbers on sites without an adult's permission?
NO
182. Does the student know to be cautious sharing their contact information on gaming sites?
YES
183. Does the student know not to exchange images or video from someone they met online?
YES
184. Does the student know to always log off when not using instant messaging?
YES
185. Do you, a parent or a trusted adult educate the student on the dangers of disclosing their personal information?
YES
186. Is the student's school websites password protected to prevent unauthorized access to the student's images?
YES
187. Is the student cautious posting online their email address to prevent screen scrapers?
YES
188. Does the student post their school name online without your permission?
NO
189. Do you, a parent or a trusted adult educate the student on the dangers of sharing personal information online?
YES
190. Do you, a parent or a trusted adult encourage the student to be cautious sharing their personal information?
YES
191. Do the student's user account names include their full or partial real name?
NO
192. Does the student post their full name or address online without a parent or your knowledge?
NO

193. Does the student know how to hide displaying their ID or personal information?
YES
194. Does the student post their email address on sites without a parent or trusted adult's permission?
NO
195. Does the student use text messaging to communicate with others you, a parent or trusted adult know?
YES
196. Does the student regularly disclose their contact information to online contacts?
NO
197. Does the student post images other than their own image?
YES
198. Does the student consistently post their full name, home address or telephone number?
NO
199. Does the student use various email addresses for different purposes?
YES
200. Do the student's email accounts have the highest level of spam filtering activated?
YES
201. Does the student post their home address on sites without a parent or your permission?
NO
202. Does the student post their image on sites without a parent or your permission?
NO
203. Does the student post their personal information without concern or caution?
NO
204. Do you, a parent or a trusted adult educate the student on being cautious sharing their contact information?
YES
205. Does the student include their contact information in their profiles or comments?
NO
206. Do you encourage a parent or trusted adult to monitor who the student allows to have their contact information?
YES
207. Does the student know how posting personal information online can hurt their reputation?
YES
208. Has the student shared confidential information to a now ex-friend online?
NO
209. Is the student careful what they tell others online?
YES
210. Does the student protect their images from strangers viewing them?
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, a parent or a trusted adult know how to check the student's internet history?
YES
212. Does the student know to consult a trusted adult if exposed to graphic content?
YES
213. Do you, a parent or a trusted adult discourage the student from being a party to cyber bullying?
YES
214. Do you, a parent or a trusted adult know how to deactivate the student's Caller ID services?
YES
215. Do you, a parent or a trusted adult know to contact the police if the student is sexually solicited online?
YES
216. Do you encourage a parent or trusted adult to set rules for the student's online activity inside and outside the home?
YES
217. Are you, a parent or trusted adult familiar with common chat room lingo used by children?
YES
218. Do you, a parent or a trusted adult know what computer safeguards the student's friends have at their homes?
YES
219. Are the student's instant messaging contacts and "buddy" lists regularly discussed and inspected?
YES
220. Do you encourage a parent or trusted adult to monitor pornographic content on the student's computer?
YES
221. Does the student have daily time limits for being online?
YES
222. Have you encouraged a parent or trusted adult to block access from the student visiting adult oriented websites?
YES
223. Do you encourage a parent or trusted adult to prohibit the student from online activity at night unless supervised?
YES

224. Do you encourage a parent or trusted adult to monitor the students’ friend lists on their social sites?
YES
225. Do you, a parent or a trusted adult engage the student in discussions about their friend’s online habits?
YES
226. Do you, a parent or a trusted adult encourage the student to tell an adult if they receive a sexual solicitation?
YES
227. Do you, a parent or a trusted adult remind the student to only download legal files, music and videos?
YES
228. Do you, a parent or a trusted adult know how to respond if the student explores sexual websites?
YES
229. Do you, a parent or a trusted adult have the appropriate contacts if the student is contacted by someone suspicious?
YES
230. Do the adults supervising the student when visiting friends have online rules?
YES
231. Do you, a parent or a trusted adult discuss with the student possible online dangerous scenarios?
YES
232. Do you, a parent or a trusted adult know how to check the student's history folder if they become suspicious?
YES
233. Do you encourage a parent or trusted adult to confirm chat rooms are always monitored by a trained moderator?
YES
234. Do you encourage a parent or trusted adult to limit the student's online chatting on their favorite gaming or club sites?
YES
235. Does the student know a parent or trusted adult visit sites they frequently visit?
YES
236. Do you encourage a parent or trusted adult to keep all ICT in a communal area of their home that is central to their view?
YES
237. Do you, a parent or a trusted adult know to contact the police if the student reports being sexually solicited online?
YES
238. Do you encourage a parent or trusted adult to set rules for the student's online activity inside and outside the home?
YES
239. Are the student's instant messaging contacts and “buddy” lists checked regularly?
YES

240. Do you encourage a parent or trusted adult to monitor the students’ 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 student spend less time with friends and more time online?
NO
242. Does the student have an online curfew?
YES
243. Does the student report he or she feels unattractive or not liked?
NO
244. Does the student appear sad or depressed?
NO
245. Does the student post comments not typical of their age online?
NO
246. Has the student withdrawn from his or her favorite activities?
NO
247. Does the student engage in risk-taking and/or self-destructive behaviors?
NO
248. Has the student had a drastic change in grades?
NO
249. Has the student been less attentive or falling behind in school?
NO
250. Has the student's behavior at home changed without explanation?
NO
251. Does the student seem distressed or anxious?
NO
252. Does the student have little adult involvement or none?
NO
253. Has the student reported a loss of appetite or lack of sleep?
NO
254. Has the student withdrawn from friends and family members?
NO
255. Does the student prefers online contacts to offline friends?
NO
256. Does the student complain about stomachaches or feeling ill?
NO
257. Do you, a parent or a trusted adult define the student as being defiant and/or oppositional?
NO

258. Has the student witnessed a traumatic event or significant adult conflict?
NO
259. Does the student report disliking school, the teachers or the students?
NO
260. Has the student reported not feeling accepted by his/her peers?
NO
261. Does the student report feeling more accepted by adults?
NO
262. Does the student appear hopeless and/or discouraged?
NO
263. Does the student become easily upset?
NO
264. Does the student spend more time online and/or uninterested in family functions?
NO
265. Does the student become easily agitated and/or externalizes blame?
NO
266. Do the student's friends have behavioral/emotional problems in school?
NO
267. Has the student had a drastic change in grades?
NO
268. Does the student have little adult involvement or none?
NO
269. Does the student report a loss of appetite or lack of sleep?
NO
270. Does the student complain about feeling overwhelmed or distressed?
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 student spend large periods online involved with social media?
NO
272. Does the student know to end online contact if someone starts with questions about sex?
YES
273. Does the student have a Facebook account a parent or trusted adult rarely inspects?
NO
274. Does the student have a social media profile with information available to the public?
NO
275. Does the student often share with others his or her social media profile?
NO

276. Do you, a parent or a trusted adult know the age restrictions of the students' favorite social media sites?
YES
277. Does the student visit chatrooms without adult moderation?
NO
278. Does the student know to be cautious of flattering messages received online?
YES
279. Does the student keep their profile pages private only for invited friends?
YES
280. Do you, a parent or a trusted adult spend time educating the student on proper online etiquette?
YES
281. Does a parent or trusted adult monitor social media sites the student frequents?
YES
282. Do you encourage a parent or trusted adult to join and become a "friend" or "buddy" on the student's profile?
YES
283. Does the student have a mobile device with an application to their social media profile?
NO
284. Does the student limit who can view images and videos on their profile page?
YES
285. Are you, a parent or trusted adult aware Facebook requires a child to be 13 years old before they can sign up?
YES
286. Do you, a parent or trusted adult review privacy and security settings on social media sites with the student?
YES
287. Does the student know social media (i.e. Facebook), when used carelessly, is dangerous?
YES
288. Do you encourage a parent or trusted adult to prohibit the student from posting their image in a public profile?
YES
289. Does the student have a Twitter account an adult does not monitor?
YES
290. Does the student allow people they do not know join their "friends" list?
NO
291. Does the student have their Facebook set to "Friends of Friends" or "Public?"
NO
292. Does the student refuse friend requests from others they do not know?
YES
293. Does the student refrain from responding to strange messages?
YES

294. Is the student respectful online and shares positive information when prompted?
YES
295. Is the student aware people they meet online may lie about who they are?
YES
296. Does the student practice caution with their social profiles?
YES
297. Does the student know to end contact if someone starts with questions about sex?
YES
298. Does the student know to be cautious of flattering messages from others they meet online?
YES
299. Do you, a parent or a trusted adult spend time educating the student on proper online etiquette?
YES
300. Do you encourage a parent or trusted adult to join and become a “friend” or “buddy” on the student's profile?
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 student give out their Social Security Number to unknown online requests?
NO
302. Does the student know what to do if receiving harassing, slandering or unwanted communication via ICT?
YES
303. Does the student know cyberstalkers pose as their victim or target and attack others online?
YES
304. Does the student know what to do if receiving unwanted emails or text messages from an ex-partner, acquaintance or stranger?
YES
305. Does the student know what to do if receiving unsolicited threatening emails and/or death threats?
YES
306. Does the student know what to do if receiving electronic viruses from an ex-partner, acquaintance or stranger?
YES
307. Does the student know what to do if receiving extreme amounts of spam from an ex-partner, acquaintance or stranger?
YES

308. Does the student know what to do if sexually harassed via online posts, emails and phone or text messages?
YES
309. Does the student know if cyber harassed, slandered or cyberbullied in chatrooms to contact a trusted adult?
YES
310. Does the student know what to do if finding personal or financial information online posted by an ex-partner, acquaintance or stranger?
YES
311. Does the student know what to do if subscribed to pornography and/or distasteful advertising without consent?
YES
312. Does the student regularly check their computers, cell phones or mobile devices for spyware?
YES
313. Does the student check their mobile devices to see if they are being tracked by GPS technology?
YES
314. Does the student check if their phone calls or messages are being intercepted?
YES
315. Does the student know what to do if being impersonated online?
YES
316. Does the student know if being cyberstalked, slandered or harassed, there is a good chance it is an ex-partner, acquaintance or peer?
YES
317. Does the student know cyberstalkers contact the victim or the target's family, employer, school and financial institution?
YES
318. Does the student know posting personal information when blogging have higher rates of cyberstalking and harassment?
YES
319. Does the student know cyberstalkers and harassers follow their victim or target from site to site?
YES
320. Does the student make sure their email addresses, instant messaging usernames and links to personal homepages cannot be connected to them?
YES
321. Does the student know online users are particularly susceptible to cyberstalking, slander and harassment if video blogging (vlogging?)
YES
322. Does the student 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 student know cyberstalkers inconspicuously pose as friends, colleagues or fans asking innocuous questions they will use to attempt recovering their target's passwords?
YES
324. Does the student know that most cyberstalking, internet slander and harassment involve someone they have interacted with in his or her recent past?
YES
325. Does the student know that cyberstalking, internet slander and harassment can occur whether the offender or target resides or works in the same location?
YES
326. Does the student 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 student know to avoid announcing their physical location via status updates of GPS-enabled applications?
YES
328. Does the student know changing Internet Service Providers and reporting aggressive events is recommended to stop cyberstalking and internet slander?
YES
329. Does a parent or trusted adult know it is recommended to contact the local FBI Computer Crimes Unit if the student is cyberstalked, threatened or harassed?
YES
330. Does the student know an unattended logged in computer should always be turned off.?
YES

Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Correct Responses__+ Does Not Apply Responses__= IPI-E 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 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.

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.