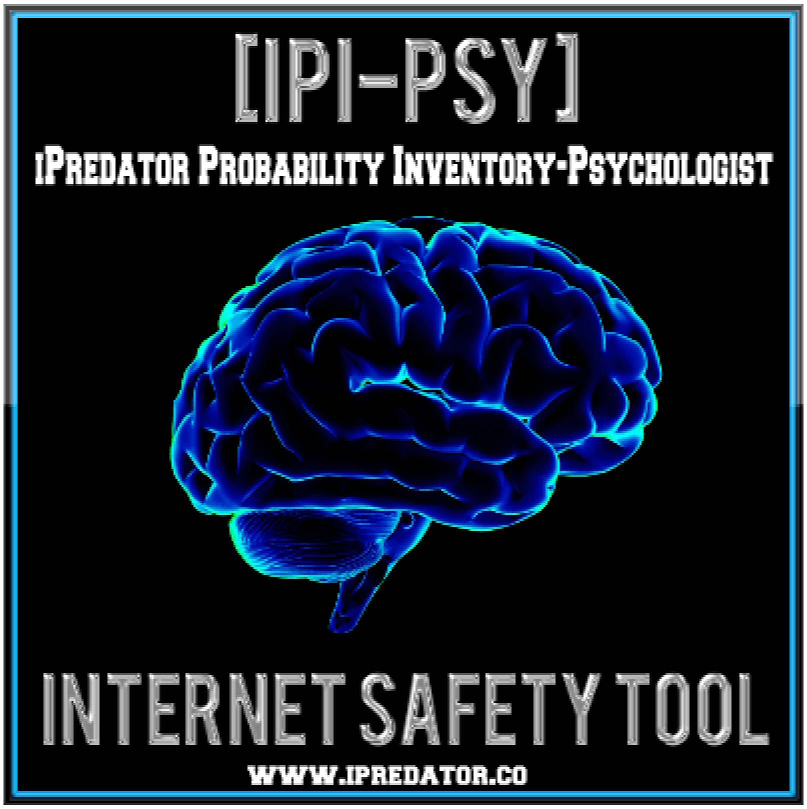
IPI-PSY

iPredator Probability Inventory - Psychologist

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



iPredator Probability Inventory - Psychologist (IPI-PSY)

The iPredator Probability Inventory - Psychologist is a 330-question data collection, educational and diagnostic tool for psychiatrists, psychologists, social workers and behavioral healthcare professionals regarding a child, adolescent or adult's online preparedness, probability and vulnerability of being cyberstalked, sexually solicited, stolen from and/or targeted by iPredators. The IPI-PSY can also be used as an adjunct to individual and group therapy, prevention education training, an adjunct to intake assessments and behavioral healthcare training.

Upon completion of the IPI-PSY, the IPI score ranges from 0-330 and represents the preparedness, vulnerability and risk potential of the subject being targeted by an iPredator and/or being an iPredator. The IPI-PSY questions are formatted to investigate the knowledge base, environmental aspects and behavioral actions necessary for Internet safety and preparedness if cyber attacked. The IPI-PSY 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 behavioral healthcare professional goals or areas of assessment. The IPI-PSY also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-PSY DIRECTIONS

1. The time required to complete the IPI-PSY 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-PSY
iPredator Probability
Inventory-Psychologist
WWW.IPREDATOR.CO

IPI-PSY

Subject's Gender: Male__ Female__
Age: Child (6-9) __Tween (10-13) __Teen (14-18) __Young Adult (19-21) __
Subject's Average Daily Online Activity: 0-1Hour__1-3 Hours__3-5 Hours__5+Hours__
IPI Respondent: Parent__ Adult__ Caregiver__Educator__Other__

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. Does anyone discuss cyberbullying or cyber harassment with the patient?
YES
2. Has the patient returned home with missing, stolen or damaged belongings due to their online activities?
NO
3. Does the patient know to ignore being harassed or teased online?
YES
4. Has the patient been flamed (a provoking message) online?
NO
5. Has the patient been harassed or taunted online about their race or sexual orientation?
NO
6. Has the patient been threatened, embarrassed or teased online about their physical attributes?
NO
7. Has the patient been negative about their job, school or their home environment related to their online activities?
NO
8. Has anyone sent or posted harmful messages about the patient online?
NO
9. Has the patient been teased or embarrassed by an online stranger?
NO
10. Has the patient had an online relationship involving an adversarial or negative outcome?
NO
11. Has the patient had secrets they have disclosed been spread by others online?
NO
12. Has anyone captured, saved or stored embarrassing information online about the patient?
NO

13. Has the patient retaliated to online information being spread about them?
NO
14. Has the patient been sexually harassed by someone online?
NO
15. Does the patient know how to respond if a friend is being cyberbullied or harassed?
YES
16. Does the patient know who, when and how to report a cyber harasser?
YES
17. Has the patient sent or received unwanted offensive online content?
NO
18. Has the patient been sexually teased or taunted online?
NO
19. Has the patient been aggressive or mean to others online?
NO
20. Would the patient be a bystander if a peer was being harassed and teased?
NO
21. Does the patient know what encourages online aggression?
YES
22. Does the patient appear sullen going to or returning from work or school?
NO
23. Does the patient know pictures they post, or share can be used to embarrass them?
YES
24. Does the patient practice good digital citizenship (online manners?)
YES
25. Does the patient know what to do if they are being taunted by others?
YES
26. Has the patient sent or received questionable information or images online?
NO
27. In the last 90 days, has someone repeatedly tease the patient online?
NO
28. In the last 90 days, has someone repeatedly lie or deceive the patient online?
NO
29. In the last 90 days, has the patient been cyberbullied or cyber harassed?
NO
30. In the last 90 days, has someone sexually harassed the patient 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 personal information about the patient?
NO

32. Is the patient cautious when posting personal information online?
YES
33. Does the patient know what “digital footprint” means?
YES
34. Has the patient shared confidential information to a now ex-friend or ex-intimate partner online?
NO
35. Does the patient practice caution what they disclose online?
YES
36. Does the patient protect their images and videos from strangers viewing them?
YES
37. Does the patient have a positive digital reputation?
YES
38. Does the patient know their photographs can remain in cyberspace for years?
YES
39. Does the patient know information shared online may be impossible to delete?
YES
40. Does the patient have a mobile device with information that is embarrassing?
NO
41. Does the patient know sexting can be criminal and shared with others?
YES
42. Does the patient know their personal information can go viral?
YES
43. Does the patient know everyone has an online digital footprint?
YES
44. Does the patient know images and videos can be reposted multiple times?
YES
45. Does the patient know what information can be harmful to their reputation?
YES
46. Does the patient take steps to ensure their digital reputation is accurate?
YES
47. Does the patient monitor what information they post?
YES
48. Has the patient practiced good behavior online and in chatrooms?
YES
49. Does the patient enter their personal information into search engines?
YES
50. Does anyone respectfully inquire about the patient’s social media profiles?
YES
51. Has the patient engaged in sexting?
NO
52. Does anyone spend time with the patient educating him or her on digital reputation?
YES
53. Does the patient know content they share online can be reposted?
YES

54. Does the patient know information shared online can hurt their future?
YES
55. Does the patient share provocative photos or details online?
NO
56. Does the patient post personal information to impress others?
NO
57. Has the patient shared privileged information to an ex-friend online?
NO
58. Is the patient careful what personal information they disclose to others online?
YES
59. Does the patient know their images and videos can stay in cyberspace for years?
YES
60. Does the patient know information about them 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 patient had sexual conversations with someone they met online?
NO
62. Did the patient have a Facebook account prior to age 13?
NO
63. Does the patient refuse to disclose websites they have visited?
NO
64. Has the patient visited, spent money or been exposed to online sex sites?
NO
65. Does the patient frequently use the internet without supervision or caution?
NO
66. Has the patient received or made phone calls to others they met from their online contacts?
NO
67. Does the patient inform online contacts when an adult or love one will not be home allowing them to chat privately online?
NO
68. Has the patient ever been contacted by an online stranger?
NO
69. Has the patient ever met someone in person he or she met online?
NO
70. Has anyone approached the patient unexpectedly and he or she shut off the computer quickly?
NO

71. Does the patient know not to respond to online strangers requesting their contact information?
YES
72. Has the patient been contacted by an online user recently introduced to them from online contacts?
NO
73. Does the patient communicate online with online strangers discussing sexual topics?
NO
74. Does the patient isolate in his or her room while online or text messaging?
NO
75. Has the patient visited chatrooms without topic restrictions or trained moderators?
NO
76. Does the patient use ICT engaging in online activity in their room during late night hours?
NO
77. Has the patient engaged in online activities they have been restricted or discouraged from by loved ones?
NO
78. Does the patient know to log out if they feel threatened, uncomfortable or fearful?
YES
79. Does the patient engage in online activities they do not want a loved one to know about?
NO
80. Would the patient meet someone they met online without a loved one knowing about the meeting?
NO
81. Does the patient know they are at a higher risk being contacted by strangers at night?
YES
82. Has the patient met someone they have met online without a loved one, despite being restricted from the meeting?
NO
83. Does the patient accept free software, ring tones or screen savers from strangers?
NO
84. Does the patient hesitate to disclose whom they converse with online?
NO
85. Does the patient have names on their "buddy" or "friend" lists a loved one does not know?
NO
86. Does the patient send personal information to others they do not know?
NO
87. Has the patient discussed sex online with people they do not know?
NO
88. Has the patient text messaged or chatted about sex online with others?
NO

89. Has the patient ever been contacted by an online stranger initiating sexual topics?
NO
90. Has the patient ever met someone in person he or she met online without telling a loved one?
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. Is the patient educated on iPredators?
YES
92. Is the patient aware that iPredators target online users using kindness and understanding?
YES
93. Is the patient aware iPredators use attention, affection and gifts to seduce online users?
YES
94. Is the patient aware most iPredators are patient and create factitious profiles?
YES
95. Does the patient know iPredators create profiles pretending to be their same age or interested in similar hobbies?
YES
96. Is the patient aware iPredators become educated in areas their targets find intriguing?
YES
97. Does the patient know the ideal age an iPredator targets are children between 11-14 years old?
YES
98. Does the patient know iPredators encourage others to add them to their “buddy” and “friend” lists?
YES
99. Does the patient know peer-to-peer networks can expose their computer or mobile devices to iPredators?
YES
100. Does the patient know the best protection from iPredators is effective online communication with loved ones?
YES
101. Does the patient know how to block sites on computers or mobile devices from being accessed by iPredators?
YES
102. Does the patient know iPredators use keywords at their sites popular to their target audience?
YES

103. Does the patient know iPredators often troll and explore sex sites and non-moderated chat rooms?
YES
104. Does the patient know iPredators are notorious for pretending to be the patient and writing to their online contacts with fake profiles?
YES
105. Is the patient educated about online sexual predators and the grooming process?
YES
106. Is the patient suspicious of anyone who encourages them online to be defiant to authority, loved ones or respected peers?
YES
107. Does the patient know iPredators encourage their targets to keep online contacts secret from loved ones or authorities?
YES
108. Does the patient know most iPredators will be encouraging, patient and reserved?
YES
109. Does the patient know iPredators offer their online accounts to potential targets to converse with as a targeting strategy?
YES
110. Does the patient know iPredators embed popular patient search terms in their sites?
YES
111. Does the patient know iPredators consistently tell their targets they are always available to them online?
YES
112. Does the patient communicate to online strangers using a false identity?
NO
113. Is the patient educated on “grooming” by iPredators in their quest to exploit children or online users?
YES
114. Does the patient know file-sharing sites allow iPredators to access portions of their ICT?
YES
115. Does the patient know iPredators encourage their targets to share their photographs?
YES
116. Does the patient know iPredators encourage their target to share confidential information?
YES
117. Does the patient know iPredators are kind and understanding to their targets?
YES
118. Does the patient know iPredators offer gifts to their targets?
YES
119. Does the patient know iPredators will try to steal their identity?
YES

120. Does the patient know iPredators create profiles pretending to be an acquaintance from their targets past?
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. Does the patient know iPredators seek targets with mobile devices available during late night hours?
YES
122. Does the patient know how to activate and deactivate their mobile device GPS services?
YES
123. Does the patient's mobile devices have unlimited text messaging and online access that they use late at night or mostly in private?
NO
124. Does the patient know to continually change the passwords to their mobile devices?
YES
125. Does the patient know how to prevent unwanted access to their mobile devices?
YES
126. Does the patient know how to track the sending and receiving of digital photos from their mobile devices?
YES
127. If the patient has a home WiFi system, do they run additional firewalls?
YES
128. Does the patient know the dangers of GPS location services?
YES
129. Does the patient know GPS location services allow anyone to know their exact location?
YES
130. Does the patient or a loved one know to contact their mobile device service about adult controls?
YES
131. Does the patient or a loved one spend time learning mobile device safety?
YES
132. Does the patient or a loved one know how to install security on their mobile devices?
YES
133. Does the patient or a loved one know about near field communications and mobile devices to make purchases?
YES

134. If the patient favors text messaging as their primary means of communicating, do they practice safe mobile device usage?
YES
135. Does the patient or a loved one know how to set up remote lock and wipe features in their mobile devices?
YES
136. Does the patient or a loved one know how to install security software in their mobile devices?
YES
137. Does the patient or a loved one know to regularly monitor stored images on their mobile devices?
YES
138. Does the patient or a loved one download and install antivirus software on their mobile devices?
YES
139. Does the patient treat their mobile devices as carefully as their wallets?
YES
140. Does the patient share confidential information with their mobile devices?
NO
141. Does the patient silence their mobile devices in public places?
YES
142. Does the patient or a loved one set age-appropriate restrictions or time limits on their mobile device usage?
YES
143. Does the patient comply with work or school policies regarding mobile device usage?
YES
144. Does the patient know there are few methods of filtering web content on mobile devices?
YES
145. Does the patient or a loved one know that pornographic content is more accessible on mobile devices?
YES
146. Does the patient or a loved one know sexting using mobile devices is a growing trend and may have criminal implications?
YES
147. Does the patient give their mobile phone passwords to a trusted loved one?
YES
148. Does the patient know how to prevent access to their mobile phone?
YES
149. Has the patient learned about the dangers of GPS location services?
YES
150. Does the patient 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. Does the patient or a loved one know they will be introduced by peers to questionable web sites?
YES
152. Does the patient know to never share his or her password with close friends?
YES
153. Does the patient know there is no filtering software that can replace adult supervision or online activity honesty with loved ones?
YES
154. Does the patient know they may accidently disclose his or her phone number if they have Caller ID?
YES
155. Does the patient have multiple passwords for different accounts?
YES
156. Does the patient know who has access to their computers and mobile device passwords?
YES
157. Does the patient enter private chat rooms?
NO
158. Has the patient been exposed to sites dealing with hatred?
NO
159. Does the patient activate their GPS services on mobile devices without informing loved ones?
NO
160. Is the patient familiar with bot software, spyware, keystroke loggers and viruses?
YES
161. Does the patient know that online gaming systems provide extensive communication features often frequented by iPredators?
YES
162. Does the patient visit adult content websites?
NO
163. Does the patient or a loved one know there is technology to identify people he or she interacts with online?
YES
164. Does the patient or a loved one set their computer and mobile device security settings on high?
YES

165. Is the patient or a loved one familiar with home wireless networks (WiFi) and their security settings?
YES
166. Does the patient participate in online activities a loved one or internet safety expert would not approve of?
NO
167. Does the patient or a loved one know Facebook is the fastest growing site and often visited by sexual predators and cyber criminals?
YES
168. Does the patient know to never click a link in an unknown email or instant message?
YES
169. Can the patient or a loved one define unintentional vs. intentional access to offensive web content?
YES
170. Does the patient know not to click on links in a video comments section?
YES
171. Does the patient or a loved one know web sites use keywords from the top twenty brand names to attract site visitors?
YES
172. Does the patient or a loved one have filters and security software installed to make some chatrooms inaccessible?
YES
173. Does the patient or a loved one know how to disable the preview function in their email?
YES
174. Does the patient or a loved one know parental control software helps limit the sites accessed?
YES
175. Has the patient or a loved one installed the appropriate security controls on their mobile devices?
YES
176. Does the patient or a loved one know some adult websites format their sites, so children or regular graphic content online users will view it?
YES
177. Does the patient or a loved one know there is no filtering software 100% successful at filtering offensive content from mobile devices?
YES
178. Does the patient or a loved one know who has access to their mobile device passwords?
YES
179. Does the patient or a loved one know online gaming systems provide extensive communication features allowing access to their contact information?
YES

180. Does the patient or a loved one know how to set their mobile device 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 patient post their home or cell phone numbers on sites?
NO
182. Does the patient know to be cautious sharing their contact information at gaming sites?
YES
183. Does the patient know not to exchange pictures from someone they met online?
YES
184. Does the patient know to always log off when not using instant messaging?
YES
185. Does the patient know the dangers of disclosing their personal information?
YES
186. Has the patient or a loved one confirmed that their work or school website is password protected?
YES
187. Is the patient cautious posting their email address to prevent "*Screenscrapers*"?
YES
188. Does the patient post their contact information online without concern?
NO
189. Is the patient educated on the dangers of sharing personal and financial information online?
YES
190. Is the patient cautious sharing their personal information in chat rooms?
YES
191. Do the patient's user account names include their full or partial real name?
NO
192. Does the patient post their full name or address when text messaging?
NO
193. Does the patient know how to hide displaying their ID or personal information?
YES
194. Does the patient post their email address on their social profiles for public display?
NO
195. Has the patient text messaged others they have never met in person?
NO
196. Does the patient regularly disclose their contact information to online contacts?
NO

197. Does the patient post profile images that will not disclose their identity?
YES
198. Does the patient consistently post their full name, home address and telephone number all together at one site?
NO
199. Does the patient use various email addresses for different purposes?
YES
200. Do the patient's email accounts have the highest level of spam filtering activated?
YES
201. Has the patient posted their home address on sites without a loved one's permission or knowledge?
NO
202. Has the patient posted their image on sites without permission or knowledge of a loved one?
NO
203. Does the patient post their personal information without concern or caution?
NO
204. Does the patient practice caution sharing their contact information online?
YES
205. Does the patient include their contact information in their profiles or comments?
NO
206. Does the patient monitor who they allow to have their contact information?
YES
207. Does the patient know how posting personal information online can hurt their reputation?
YES
208. Has the patient shared confidential information to a now ex-friend online?
NO
209. Is the patient careful what they disclose to others online?
YES
210. Does the patient 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. Does the patient protect their personal information from other online users?
YES
212. Does the patient know to consult a professional or loved one if sent graphic or disturbing online content from someone they never met?
YES

213. Does the patient encourage their peers to engage cyber bullying, cyber harassment or cyber stalking?
NO
214. Does the patient know how to deactivate their Caller ID services?
YES
215. Does the patient know to contact the police if they are sexually solicited online without their consent?
YES
216. Does the patient have rules they have set for themselves regarding online activity inside and outside the home?
YES
217. Is the patient familiar with common chat room lingo?
YES
218. Does the patient know what computer safeguards their peers have at their homes or on their mobile devices?
YES
219. Is the patient's instant messaging contacts and “buddy” lists checked regularly?
YES
220. Does the patient share or discuss pornographic content on their computer or mobile devices to online strangers?
NO
221. Does the patient have daily time limits for being online?
YES
222. Does the patient know the dangers of visiting adult oriented web sites?
YES
223. Does the patient engage in adult content chat rooms?
YES
224. Does the patient monitor their friend lists on social networking sites?
YES
225. Does the patient engage in discussions about their online habits?
YES
226. Does the patient know to tell a loved if they receive a sexual solicitation or disturbing information from an online stranger?
YES
227. Does the patient only download legal files, music and videos?
YES
228. Does the patient know how to respond if sent sexual or offensive content from online strangers?
YES
229. Does the patient know what to do if contacted by someone suspicious?
YES
230. Does the patient, when visiting peers, practice appropriate online rules?
YES
231. Does the patient know how to respond to dangerous online scenarios?
YES

232. Does the patient clear their history folder if a loved becomes suspicious of their online activities?
NO
233. Does the patient confirm chat rooms are always monitored by a trained moderator?
YES
234. Does the patient know to be cautious of online chatting when visiting their favorite gaming or club sites?
YES
235. Does the patient visit websites or chatrooms offensive to others?
NO
236. Does the patient keep all their information and communications technology up to date with security features?
YES
237. Does the patient know whom to contact if their identity has been stolen online?
YES
238. Does the patient know the consequences of using the internet in an unsafe manner?
YES
239. Does the patient regularly check and filter their instant messaging contacts and buddy lists?
YES
240. Does the patient know how to combat the latest cyber threats?
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 patient spend less time with friends and more time online?
NO
242. Does the patient have a personal online curfew or online time limits?
YES
243. Does the patient report feeling unattractive due to their online activities?
YES
244. Does the patient appear sad or depressed due to their online activities?
NO
245. Does the patient post online comments not typical of their age or maturity level?
NO
246. Has the patient withdrawn from his or her favorite activities?
NO
247. Does the patient engage in risk-taking or self-destructive behaviors?
NO

248. Has the patient had a drastic change in grades or work performance due to their online activities?
NO
249. Has the patient been less attentive or falling behind in school or work objectives due to their online activities?
NO
250. Has the patient's behavior at home changed without explanation due to their online activities?
NO
251. Does the patient report feeling distressed or anxious due to their online activities?
NO
252. Does the patient have little social involvement or none due to their online activities?
NO
253. Has the patient reported a loss of appetite or lack of sleep due to their online activities?
NO
254. Has the patient withdrawn from peers and family members due to their online activities?
NO
255. Does the patient have few offline peers and prefers online contacts?
NO
256. Does the patient complain about stomachaches or feeling ill due to their online activities?
NO
257. Do others define the patient as being defiant or oppositional?
NO
258. Has the patient witnessed a traumatic event or sustained conflict?
NO
259. Does the patient report disliking school, work or loved ones due to their online activities?
NO
260. Has the patient reported not feeling accepted by his/her peers?
NO
261. Does the patient report feeling more accepted by their chatroom or online contacts?
NO
262. Does the patient appear hopeless or discouraged due to their online activities?
NO
263. Does the patient become easily upset?
NO
264. Does the patient appear or report being uninterested in family functions due to their online activities?
NO
265. Does the patient become easily agitated or externalizes blame due to their online activities?
NO

266. Do the patient's peers have behavioral/emotional problems in school or work due to their online activities?
NO
267. Has the patient had a drastic change in grades or financial responsibilities due to their online activities?
NO
268. Does the patient have little social involvement other than online relationships?
NO
269. Has the patient reported a lack of sleep due to their online activities?
NO
270. Has the patient neglected school, work or family responsibilities due to their 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 patient spend large periods online involved with social media?
NO
272. Does the patient know to end contact if an online stranger starts asking questions about sex?
YES
273. Does the patient have a social account loved ones are unaware of or do not monitor if the patient is a minor?
NO
274. Does the patient have a social media profile with information available to the public?
NO
275. Does the patient often share with others his/her social media profile?
NO
276. Does the patient have social media guidelines on what is permissible to share online?
YES
277. Has the patient visited chatrooms without a trained moderator?
NO
278. Does the patient know to be cautious of flattering messages from online strangers?
YES
279. Does the patient keep their profile pages "private only" for invited friends?
YES
280. Does the patient practice proper online etiquette?
YES
281. Does a loved one or trusted peer know the social media sites the patient frequents?
YES

282. Does a loved or trusted peer join and become a "friend" or "buddy" on the patient's profile?
YES
283. Does the patient have a mobile device with an application for their social media profile that they habitually check throughout their day?
NO
284. Does the patient limit who can view their photos and videos on social sites?
YES
285. Does the patient know links in tweets, posts, and online advertising are often the way cyber criminals compromise their victim's computer?
YES
286. Has the patient reviewed privacy and security settings on social media sites?
YES
287. Does the patient know social media (i.e. Facebook), when used carelessly, is dangerous?
YES
288. Does the patient know the dangers of posting their picture at a public profile?
YES
289. Does the patient review their social networking site's safety notifications, standards, and learn how to report violating content?
YES
290. Does the patient allow people they do not know join their friends list?
NO
291. Does the patient have their Facebook set to "*Friends of Friends*" or "*Public*"?
NO
292. Does the patient refuse friend requests from others they do not know?
YES
293. Does the patient refrain from responding to strange messages?
YES
294. Is the patient respectful online and shares positive information when prompted?
YES
295. Is the patient aware people they meet online may lie about who they are?
YES
296. Has the patient practiced caution with his or her social profiles?
YES
297. Does the patient know to end contact if an online stranger starts asking disturbing questions?
YES
298. Does the patient take online precautions to prevent possible negative outcomes?
YES
299. Does the patient know about and practice netiquette?
YES
300. Does the patient understand that the lack of physical interaction online provides a false sense of security?
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 patient give out their Social Security Number or Tax ID to unknown online requests?
NO
302. Does the patient know what to do if receiving harassing, slandering or unwanted communication via ICT?
YES
303. Does the patient know cyber stalkers misrepresent their identities and motives?
YES
304. Does the patient know what to do if receiving unwanted emails or text messages from an ex-partner, acquaintance or stranger?
YES
305. Does the patient know what to do if receiving unsolicited threatening emails or death threats?
YES
306. Does the patient know what to do if receiving electronic viruses from an ex-partner, acquaintance or stranger?
YES
307. Does the patient know what to do if receiving extreme amounts of spam from an ex-partner, acquaintance or stranger?
YES
308. Does the patient know what to do if sexually harassed via online posts, emails and text messages?
YES
309. Does the patient know what to do if cyber harassed, slandered or cyber bullied in chat rooms or forum posts?
YES
310. Does the patient know what to do if they find their personal or financial information posted online by an ex-partner, acquaintance or stranger?
YES
311. Does the patient know what to do if they are subscribed to pornographic websites without their knowledge or consent?
YES
312. Does the patient regularly check their computers, cell phones or mobile devices for spyware?
YES
313. Does the patient check their mobile devices for tracking GPS technology?
YES

314. Has the patient checked if their phone calls or messages are being intercepted?
YES
315. Does the patient know what to do if being impersonated online?
YES
316. Does the patient know if they are being cyber stalked or harassed, there is a good chance it is an ex-partner, acquaintance or peer?
YES
317. Does the patient know cyber stalkers contact the victim or target's family, employer, school and financial institution?
YES
318. Does the patient know posting personal information when blogging have higher rates of cyber stalking and harassment?
YES
319. Does the patient know cyber stalkers and harassers follow their victim or target from site to site?
YES
320. Does the patient make sure their email addresses, instant messaging usernames and links to personal homepages cannot be connected to them?
YES
321. Does the patient know online users are particularly susceptible to cyber stalking, slander and harassment if video blogging (vlogging?)
YES
322. Does the patient 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 patient know cyber stalkers inconspicuously pose as friends or loved ones asking innocuous questions they will use to attempt recovering their target's passwords?
YES
324. Does the patient know that cyberstalking, internet defamation and harassment usually involve someone they know?
YES
325. Does the patient know that cyber stalking, internet slander and harassment can occur whether the offender or target resides or works in the same location?
YES
326. Does the patient know a cyber stalker can be an egotistic aggressor who wants to show-off to their peers, online peers or colleagues?
YES
327. Does the patient know to avoid announcing their physical location via status updates of GPS-enabled applications?
YES
328. Does the client or loved one know changing Internet Service Providers and reporting hostile events is recommended to stop cyberstalking or internet defamation?
YES

329. Does the client or loved one know it is recommended to contact the local FBI Computer Crimes Unit if cyberstalked, threatened or harassed?
YES
330. Does the patient know an unattended logged in computer can be hazardous?
YES

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

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