ISCP

Internet Safety Checklist-Psychologist

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

Internet Safety Checklist Psychologist (ISCP)

The Internet Safety Checklist Psychologist is a 330-item checklist data collection and diagnostic tool for behavioral healthcare professionals. The goal of the ISCP is to verify a child, adolescent or adult's online preparedness and vulnerability of being cyberbullied, cyberstalked, sexually solicited, stolen from and/or victimized by iPredators. The ISCP can be used as an adjunct to individual and group therapy & prevention education training.

The ISCP is designed for online users ages 11+. Given the rapid growth of information and communications technology, the ISCP is vital to behavioral healthcare professionals in their diagnosis, treatment and discharge planning.

In addition to a data collection tool, the ISCP has been designed to allow behavioral healthcare professionals to engage in a dialogue with clients about their online practices. The ISPC also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

ISCP Directions

1. The time required to finish the ISCP averages 90-120 minutes for the 330-item checklist.

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 questions you are positive about or almost certain in your decision with minimal doubt.

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 an inventory question discusses mobile devices, but you do not own a mobile device, you would respond with choice D. Does Not Apply, Not Applicable or Not Relevant.

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__ (Does Not Apply, Not Applicable, Not Relevant) responses and compare your score to the scoring key including in your checklist packet.

7. Prior to taking the checklist, please review to the two definitions listed below and refer to them is needed. The definition of Information and Communications Technology (ICT) and iPredator is 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.

ISCP
Internet Safety Checklist Psychology

Subject's Gender: Male__Female__
Age: Child (6-9) __Teen (10-18) __Young Adult (19-21) __ Adult (22+) __
Subject's Average Daily Online Activity: 0-1Hour__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. A loved one and/or behavioral healthcare professional intermittently discusses online assailants with the client
2. The client has not returned home with missing or damaged belongings related to their online activities.
3. The client knows to ignore being harassed and teased online.
4. The client has not been persistently "*Flamed*" (online provocation).
5. The client has not been taunted online about their race or sexual orientation.
6. The client has not been threatened, embarrassed or teased online about their physical attributes.
7. The client has not been negative about school, job and/or their home environment related to their online activities.
8. Other online users have not sent or posted hostile messages about the client.
9. The client has not been teased or embarrassed by an online stranger.
10. The client has not had an online relationship involving an adversarial and/or negative outcome.
11. The client has not had secrets disclosed by others online.
12. Other online users have not captured, saved or stored embarrassing online information about the client.
13. The client has not retaliated to online information being spread about them.
14. The client has not been repeatedly harassed or berated by others online.
15. The client knows how to respond if a friend or loved one is being cyberbullied.
16. The client knows who, when and how to report a cyberbully or online assailant.
17. The client has not been sent unwanted & offensive online content.
18. The client has not been sexually teased or taunted online.
19. The client has not been aggressive and/or mean to others online.
20. The client would not be a bystander if a friend or loved one were being cyber harassed or teased.
21. The client knows what encourages a cyberbully and online assailant.
22. The client does not feel sad or angry going to or returning from school or work due to their online activities.
23. The client knows images they post or share online can be used to embarrass them.
24. The client practices good "*Digital Citizenship*".

25. The client knows what to do if others online are taunting them.
26. The client has not sent offensive content to others online.
27. In the last 90 days, online users have not repeatedly teased the client.
28. In the last 90 days, online users have not repeatedly lied to the client.
29. In the last 90 days, the client has not been cyberbullied and/or cyber harassed.
30. In the last 90 days, online users have not repeatedly harassed the client.

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. Other online users have never posted embarrassing information about the client.
32. The client is cautious when posting personal information online.
33. The client knows what "*Digital Footprint*" means.
34. The client has not shared confidential information to a now ex-friend or ex-intimate partner online.
35. The client is cautious about what they share online.
36. The client protects their images from strangers viewing the client online.
37. The client knows how to sustain and monitor a positive "*Digital Reputation*".
38. The client knows their content & images can remain in cyberspace for years.
39. The client knows information shared online may be impossible to delete.
40. The client does not have a mobile device with information that is embarrassing.
41. The client knows "*Sexting*" can be criminal and shared with others without their consent.
42. The client knows their personal information posted or shared online can go viral.
43. The client knows everyone has a "*Digital Footprint*".
44. The client knows images and videos can be reposted multiple times.
45. The client knows what information can be harmful to their "*Digital Reputation*".
46. The client and loved ones take steps to ensure their "*Digital Reputation*" is accurate.
47. The client and loved ones respectfully monitor what information they post.
48. The client practices good behavior online and in chat rooms.
49. The client intermittently enters his/her personal information into search engines.
50. The client's loved ones respectfully inquire about the client's email and social media profiles.
51. The client has not engaged in sexting with an online stranger or adversarial ex-partner.
52. Loved ones or a professional spend time with the client educating or discussing with them their "*Digital Reputation*".
53. The client knows content they share online can be used to steal their identity.
54. The client knows information shared online can hurt their future.
55. The client does not share provocative images or details online.
56. The client does not post personal information to impress others online.
57. The client has not shared sensitive information to an ex-friend or ex-partner online.
58. The client is careful what they disseminate online.
59. The client knows their images and videos can stay in cyberspace for years.
60. The client knows their personal information may be impossible to delete.

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 ICT BEHAVIORS

61. The client does not have sexual conversations with someone they met online.
62. The client has not had a social networking account prior to age 13.
63. The client discloses websites they have visited, if requested, to loved ones.
64. The client does not habitually visit pornography websites.
65. The client does not use the internet without loved ones familiar with their online activities.
66. The client has not contacted online strangers that loved ones do not know about.
67. The client does not tell online contacts when a loved one will not be home.
68. An online stranger has not contacted the client.
69. The client has not met anyone in person he or she met online without loved ones knowing.
70. Someone has not approached the client and they quickly shut off their device.
71. The client refrains from sharing personal information in anonymous chat websites.
72. The client has not accepted a phone calls from online strangers.
73. The client does not communicate with online contacts that loved ones do not know.
74. The client does not isolate in his or her room or a secluded location while online.
75. The client does not visit chat rooms without a trained moderator.
76. The client does not engage in online activity in their room and/or undisclosed location without permission or acknowledgment from loved ones.
77. The client has not been accused of engaging in cyberstalking or online trolling.
78. The client knows to log out if they feel uncomfortable or fearful.
79. The client does not engage in online activities they would not want a loved one to know about.
80. The client does not habitually go online when intoxicated.
81. The client knows they are at a higher risk being contacted by online strangers late at night.
82. The client has not met and online stranger in person without informing a loved one.
83. The client does not accept free software, ring tones or screen savers from online strangers.
84. The client does not hesitate to disclose to loved ones who they converse with online.
85. The client does not have names on their "buddy" or "friend" lists that loved ones do not know.
86. The client does not send personal information to online strangers.
87. The client has not discussed sex and/or violent topics with people they have met online.
88. The client has not text messaged or chatted about sex with online strangers.
89. The client has not been contacted by webcam from an online stranger.
90. The client has not been confronted about spending too much time engaged in online gaming.

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. The client has been adequately educated on iPredators.
92. The client is aware iPredators target online users using kindness and understanding.
93. The client is aware iPredators use attention and gifts to seduce online users.
94. The client is aware most iPredators have fake profiles.
95. The client knows iPredators create profiles pretending to be their same age with similar hobbies.
96. The client is aware iPredators are educated in areas that their targets are intrigued by.
97. The client is aware iPredators frequent anonymous chat websites and chat rooms.
98. The client knows iPredators encourage others to add them to their "friend" or "buddy" lists.
99. The client knows peer-to-peer networks can expose them to iPredators.
100. The client knows the best protection from iPredators is internet safety and "*Digital Citizenship*".
101. The client and/or loved ones know how to block sites on their devices from being accessed by iPredators.
102. The client knows iPredators use keywords in their sites popular to the online users they are targeting.
103. The client is educated on how iPredators engage in "*Identity Theft*".
104. The client knows many iPredators impersonate others.
105. The client is educated on iPredators and the "*Grooming*" process.
106. The client is suspicious of anyone who encourages them to be defiant to authority.
107. The client knows iPredators encourage targets to keep their contacts secret.
108. The client is aware many iPredators will be encouraging, patient and reserved.
109. The client is aware iPredators may offer their target gifts.
110. The client is aware some iPredators manipulate their target by being overly supportive.
111. The client is aware iPredators consistently tell their target that they are always available to chat.
112. The client knows about "*Phishing*".
113. The client is educated on "*Grooming*" by iPredators to exploit online users.
114. The client knows file-sharing sites allow iPredators to access portions of their device.
115. The client knows iPredators encourage their target to share their images online.
116. The client knows iPredators encourage their target to share confidential information.
117. The client knows iPredators are kind and understanding.
118. The client knows iPredators offer favors to their target.
119. The client knows iPredators will try to steal their identity.
120. The client knows iPredators create profiles pretending to know their peers.

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. The client is educated on the safe and secure usage of mobile devices.
122. The client knows online users must be 18 years old or knows how to activate their GPS services.
123. The client knows the potential danger of mobile devices with unlimited text messaging and online access.
124. A loved one knows the passwords to the client's mobile devices.
125. The client and/or loved ones know how to prevent unwanted access to their mobile devices.
126. The client or a loved one knows how to track the sending of digital images from the client's mobile devices.
127. If the client or loved ones have a home WiFi system, they run additional firewalls.
128. The client is educated on the dangers of GPS location services.
129. The client knows GPS location services allow anyone to know their exact location.
130. The client or loved ones have contacted the client's mobile device service about adult controls and/or security settings.
131. The client and/or loved ones spend time learning "*Mobile Device Safety*".
132. The client and/or loved ones know how to install security on the client's mobile devices.
133. The client has not been frequently confronted about spending too much time on their mobile device.
134. The client is always aware of the location of his/her mobile devices.
135. The client and/or loved ones know how to set up remote lock and wipe features in their mobile devices.
136. The client and/or loved ones know how to install security software on their mobile devices.
137. The client and loved ones regularly monitor the stored images on their mobile devices.
138. The client or loved ones have antivirus software on their mobile devices.
139. The client knows to treat their mobile devices as carefully as their wallets.
140. The client is cautious sharing privileged information using their mobile devices.
141. The client knows to silence their mobile devices in public places.
142. Loved ones set age-appropriate restrictions on the client's mobile device.
143. The client complies with school or work policies regarding mobile device usage.
144. The client is aware there are few methods of filtering web content on mobile devices.
145. Loved ones are aware that pornographic content is more accessible on mobile devices.
146. The client is aware a trend for online users is "*Sexting*" using their mobile devices.
147. The client gives their mobile phone passwords to loved ones.
148. The client and/or loved ones know how to prevent access to their mobile phone.
149. The client has learned about the dangers of GPS location services.
150. The client knows GPS location services allow anyone to know their exact location.

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. The client knows he/she will be introduced to questionable websites by peers.
152. The client knows to never share his or her passwords with friends.
153. The client knows there is no filtering software that can replace adult supervision or open communication.
154. The client knows he/she may accidentally disclose their phone number by "*Caller ID*".
155. The client knows it is beneficial to have multiple passwords.
156. A loved one is aware the client has access to their friends' internet enabled devices.
157. Loved ones or a professional discourages the client from entering private chat rooms.
158. A loved one is aware the client may be exposed to sites dealing with hatred.
159. Loved ones or a professional discourages the client from activating their geolocation services.
160. The client is familiar with bot software, spyware, keystroke loggers and viruses
161. The client knows that online gaming systems provide extensive communication features.
162. Loved ones are prepared for the client visiting adult content websites.
163. The client is knowledgeable about how cybercriminals hack their devices.
164. The client and/or loved ones know how to set a computer's security settings on "high".
165. The client is familiar with home wireless networks (WiFi) and their security settings.
166. The client does not participate in online activities a loved one does not approve of.
167. The client knows iPredators most often frequent the most popular social networking sites.
168. The client knows to never click a link in an unknown email.
169. The client know how to prevent "*Sextortion*".
170. The client does not click on the links in the video comments section.
171. The client is aware iPredators use keywords in their websites from the top twenty brand names used by online users.
172. The client or loved ones know how to install filters and security software making offensive chat rooms inaccessible.
173. The client and/or loved ones know how to disable the preview function in the client's email.
174. The client and/or loved ones know parental control software helps limit the sites the client can access.
175. The client or loved ones have installed the appropriate security controls on the client's mobile devices.
176. The client is aware adult (pornographic) websites format their sites so online users are enticed to visit.
177. The client knows there is no filtering software that can replace honest disclosure of their online activities.
178. A loved one is aware the client has access to their friends' computers and mobile devices.

179. The client knows that online gaming systems provide extensive communication features.
180. The client knows how to set their mobile device security settings on "high".

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. The client does not post their home or cell phone numbers on anonymous chat websites.
182. The client knows to be cautious sharing their contact information on gaming sites.
183. The client does not exchange images from someone they met online.
184. The client knows to always log off when not using instant messaging.
185. Loved ones or a professional educate the client on the dangers of disclosing their personal information.
186. The client has confirmed their school or work website is password protected.
187. The client is cautious posting their email address to prevent "*Screen Scrapers*".
188. The client posts their school or work name online with caution.
189. Loved ones or a professional discusses with the client the dangers of sharing personal information online.
190. Loved ones or a professional encourage the client to be cautious sharing their personal information in chat rooms.
191. The client's user account names do not include their full or partial real name.
192. The client does not post their full name or address without a loved one's knowledge.
193. The client and/or loved ones know how to hide displaying their ID or personal information.
194. The client does not share their email address in anonymous chat or video sites.
195. The client does not use text messaging to communicate with others that loved ones do not know.
196. The client does not disclose their contact information to online strangers introduced to them by others they have met online.
197. The client posts other images when prompted to post their own image if not business and/or fan pages.
198. The client does not post their home address online.
199. The client uses various email addresses for different purposes.
200. The client's email accounts have the highest level of spam filtering activated.
201. The client does not post their day-to-day activities on public sites and/or their social networking accounts.
202. The client is cautious posting their personal images online.
203. The client does not post or shares their personal information without concern or caution.
204. Loved ones or a professional educates the client on being cautious about sharing their contact information.
205. The client does not include contact information in their profiles or comments.

206. A loved one monitors and/or discusses who the client allows to have their contact information.
207. The client knows how posting personal information can hurt their reputation.
208. The client has not shared confidential information to a now ex-friend or ex-partner online.
209. The client is careful what they disclose to others online.
210. The client protects their images from online strangers viewing them.

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. The client and/or loved ones know how to check their internet history.
212. The client knows to consult a trusted adult if exposed to graphic or offensive content.
213. Loved ones or a professional discourages the client from being a bystander to cyberbullying.
214. The client and/or loved ones know how to deactivate their Caller ID services.
215. The client knows to contact the police if the client is sexually solicited online.
216. A loved one set rules or discusses with the client their online activities inside and outside the home.
217. The client is familiar with common chat room lingo used by online users.
218. The client knows what internet safeguards their friends have at their homes.
219. The client has instant messaging contacts and buddy lists are regularly inspected.
220. The client is honest to discuss their time spent online if viewed as addictive.
221. The client does not have a social networking site profile set to “public” for anyone to view is it is not career related.
222. The client would not become overwhelmed if cyber-attacked.
223. The client would not visit high-risk websites (i.e. pornographic, racist, violent) and post their contact information.
224. The client knows iPredators will encourage their targets to add them to their "buddy" and "friends" lists.
225. The client and loved ones engage in discussions about their peers’ online habits.
226. Loved ones encourage the client to tell a loved one if they get an online sexual solicitation.
227. The client only downloads legal files, music and videos.
228. A loved one knows how to respond if the client is sent offensive websites.
229. The client has the appropriate contacts if contacted by someone suspicious.
230. The client, when they visit friends, knows their online rules.
231. Loved ones discuss with the client possible online dangerous scenarios.
232. A loved one knows how to check the client's history folder if they become suspicious.
233. The client only visits chat rooms monitored by a trained moderator.
234. A loved one knows to limit or inquire about the client's chatting on their favorite online gaming or club sites.
235. The client knows loved ones may visit some, if not all, sites they frequently visit.

236. The client has all their ICT in a communal area of the home that is central to loved ones' view.
237. The client knows to contact the police if he/she is being sexually solicited online.
238. The client has self-imposed rules for their online activity inside and outside the home.
239. The client's instant messaging contacts, "friend" and "buddy" lists are checked regularly.
240. The client is skilled at protecting their ICT from iPredators.

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 FACTORS

241. The client spends more time with friends and/or coworkers and less time online.
242. The client knows it is healthy to have an online curfew.
243. The client will confide in a loved one if he or she feels unattractive or targeted.
244. The client knows to report to a trusted adult if he or she feels sad or depressed related to their online activities.
245. The client posts comments online typical of his/her age and maturity level.
246. The client has not withdrawn from his or her favorite hobbies due to their online activities.
247. The client does not engage in risk-taking and/or self-destructive behaviors online.
248. The client has not had a drastic change in grades due to their online activities.
249. The client has not been less attentive or falling behind in school or work due to their online activities.
250. The client's behavior at home, work and/or school has not changed related to their online activities.
251. The client does not seem distressed or anxious related to their online activities.
252. The client does not have minimal human involvement due to their online activities.
253. The client has not reported a loss of appetite or lack of sleep related to their online activities.
254. The client has not withdrawn from friends and family members related to their online activities.
255. The client does not have few offline friends and prefers online contacts.
256. The client does not complain about feeling afraid related to their online activities.
257. Loved ones do not define the client as being defiant and/or oppositional related to their online activities.
258. The client has not witnessed a traumatic event or significant adult conflict and shared this information online.
259. The client has not reported disliking work or school due to their online activities.
260. The client does not report feeling unaccepted by his/her peers due to their online activities.
261. The client has not reported feeling more accepted by online contacts rather than offline peers.

262. The client does not appear hopeless and/or discouraged related to their online activities.
263. The client does not become easily upset after being online.
264. The client does not spend more time online appearing uninterested in family functions, school or work activities.
265. The client does not become easily agitated and/or externalizes blame related to their online activities.
266. The client's friends do not have behavioral/emotional problems due to their online activities.
267. The client has not had a drastic change in grades or work performance due to their online activities.
268. The client has not been confronted by loved ones due to their online activities.
269. The client has not reported a loss of appetite or lack of sleep due to their online activities.
270. The client does not complain about stomachaches or feeling ill due to their online activities.

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. The client does not spend large periods online involved with social networking sites that are not academic or career related.
272. The client knows to end contact if someone asks questions about sex.
273. The client does not have social accounts they rarely discuss with loved ones.
274. The client does not have a social media profile with information available to the public.
275. The client does not share his/her social media passwords with acquaintances.
276. The client knows the privacy policies of their favorite social media sites.
277. The client does not visit chat rooms that share offensive or graphic information.
278. The client knows to be cautious of flattering messages received online.
279. The client knows to keep their social profile pages "*friends only*" for invited friends or loved ones.
280. Loved ones or a professional spend time educating the client on proper online etiquette.
281. Loved ones monitor and/or inquiries about the social media sites the client frequents.
282. A loved one has joined and become a "*friend*" or "*buddy*" on the client's social profiles.
283. The client does not have a mobile device with an application to their social media profile they use habitually.
284. The client limits those who can view images and videos on their profile page.
285. The client knows most social media sites requires a child to be 13 years old before joining.
286. The client and/or loved ones review the privacy and security settings on social media sites.
287. The client knows social media, when used carelessly, is dangerous.

288. The client does not post their images at a public profile.
289. The client does not have a social account that loved ones do not monitor and/or know about.
290. The client refrains from adding online strangers to their "friend" or "buddy" lists.
291. The client does not have a social media profile set to “public”.
292. The client refuses "friend" or "buddy" list requests from online users introduced to them by others they have met online.
293. The client refrains from responding to strange email messages.
294. The client is respectful online and shares positive information when prompted.
295. The client is aware people they meet online may lie about their identity.
296. The client practices caution with their social profiles.
297. The client is aware online users engaged in nefarious activities frequent video chat sites.
298. The client knows to be cautious of flattering messages from online acquaintances.
299. The client and loved ones spend time discussing proper online etiquette.
300. A loved one has joined and become a "friend" or "buddy" on the client's social profiles.
301. The client does not give out their social security number to unknown online requests.

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

302. The client knows what to do if they receive harassing, slandering or unwanted communication online.
303. The client knows cyberstalkers impersonate their target to attack others.
304. The client knows what to do if they receive unwanted emails or text messages from an ex-partner, acquaintance or stranger.
305. The client knows what to do if they receive unsolicited threatening emails and/or death threats.
306. The client knows what to do if they receive electronic viruses from an ex-partner, acquaintance or stranger.
307. The client knows what to do if they receive spam from an ex-partner, acquaintance or stranger.
308. The client knows what to do if sexually harassed via online posts, emails, phone or text messages.
309. The client knows what to do if cyber harassed, slandered or cyberbullied in chat rooms.
310. The client knows what to do if they find their personal or financial information posted online by an ex-partner, acquaintance or stranger.
311. The client knows what to do if subscribed to pornography and/or distasteful advertising without their consent.
312. The client knows to regularly check their computers and mobile devices for spyware.
313. The client and/or loved ones know how to check if their mobile devices are being tracked by GPS technology.

314. The client and/or loved ones know how to check if their phone calls are being intercepted.
315. The client knows what to do if being impersonated online.
316. The client knows if being cyberstalked, slandered or harassed, there is a good chance it is an ex-partner, acquaintance or peer.
317. The client knows cyberstalkers contact the victim or target's family, employer, school or work and financial institution.
318. The client knows online users who post personal information, when blogging, have higher rates of cyber stalking and harassment.
319. The client knows cyberstalkers and harassers follow their target from site to site.
320. The client knows to make sure their email addresses, instant messaging usernames and links to personal homepages cannot be connected to them.
321. The client knows online users are particularly susceptible to cyberstalking, slander and harassment if video blogging (vlogging).
322. The client knows a cyberstalker can be an obsessed love interest or someone with a grudge due to a minor or imagined reason.
323. The client knows cyberstalkers inconspicuously pose as friends or coworkers asking innocuous questions they will use to recover their passwords.
324. The client knows that most cyberstalking, internet slander and harassment involves defaming their character and/or seeking to control or manipulate their target.
325. The client knows that cyberstalking can still occur when the assailant and target resides in various locations.
326. The client knows a cyberstalker or troll can be an egotistic aggressor who wants to show-off to online peers.
327. The client knows to avoid announcing their physical location via status updates on GPS-enabled applications.
328. The client knows cyberstalking involves direct or indirect online physical threats.
329. The client knows to contact their local FBI Computer Crimes Unit if cyberstalked or physically threatened online.
330. The client knows an unattended internet enabled device should be turned off.

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

Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Yes Answers__ + Does Not Apply__ = ISCP Score__

ALL CORRECT RESPONSES ARE A. Y__ (Yes, Agree, True)

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.

(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 the ISCP 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.

Although obtaining a high score indicates a minimal probability of a damaging cyber-attack, it is still always crucial to be alert and prepared to defend against iPredators as they change their tactics paralleling advancements in technology. 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, 0-100 or 0-330 depending on the IISC assessment. In this formula, the score represents the risk potential and vulnerability of the Online user, the business or the subject being queried from being targeted by a cyberbully, cyberstalker, cybercriminal, nefarious corporate competitor or online sexual predator. Whether taken one time or on multiple occasions, the goal is to finish with a score in the top 10% of all the IISC assessments.

IISC SCORING KEY

Internet Safety Checklist Psychology
ISCP

Note: Just as all the IISC tools, it is recommended to take the ISCP on a quarterly basis. The goal for optimal internet safety & cyber security functioning is to score a 300 or higher. "IDK" & wrong responses should be addressed immediately with a structured plan of action. If and/or when you score a 300 or higher, you are skilled in internet safety strategies and understand the dangers that lurk in cyberspace. You, the business being assessed or the subject you are assessing are encouraged to educate others in your community.

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.

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.

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.

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.

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

Score: (250-299)
Category: Skilled iPredator Protected Online User.
Risk Potential: Mild.
iPredator Involvement: Possible, but Unlikely.
Intervention Plan: Continue iPredator Protection & Prevention Strategies.
Level of Urgency: Not Urgent, Important to Address if Scored (250-270).

Score: (300-330)
Category: Advanced iPredator Protected Online User.
Risk Potential: Minimal.
iPredator Involvement: Unlikely.
Intervention & Education Plan: Consider Educating Others.
Level of Urgency: 0%, All iPredator Issues Addressed.

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist, cyberpsychology researcher and online safety educator. In 2009, Dr. Nuccitelli finalized his dark side of cyberspace concept called iPredator. Since 2010, he has advised those seeking information about cyberbullying, cyberstalking, cybercriminal minds, internet addiction and his Dark Psychology concept. By day Dr. Nuccitelli is a practicing psychologist, clinical supervisor and owner of MN Psychological Services, PLLC. After work and on the weekends, he volunteers helping online users who have been cyber-attacked. Dr. Nuccitelli's is always available to interested partied and the media at no cost. The iPredator website and everything created by Dr. Nuccitelli is educational, free and public domain.