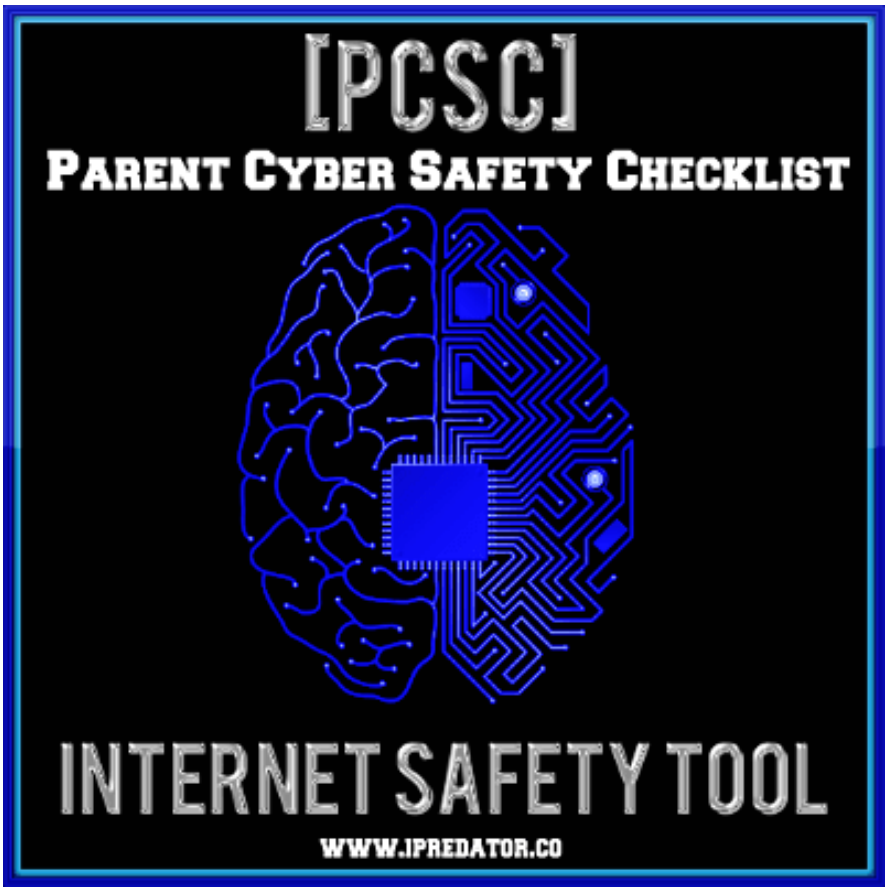
PCSC

Parent Cyber Safety Checklist

Michael Nuccitelli, Psy.D.
347-871-2416 New York, New York
www.ipredator.co



Parent Cyber Safety Checklist (PCSC)

The Parent Cyber Safety Checklist is a 330-item education, assessment and data collection checklist designed for parents and primary caregivers on pre-pubescent and adolescent internet safety and responsible internet enabled device usage. The PCSC is constructed for parents and primary caregivers to verify and confirm their child's internet safety practices are valid in preventing a cyber-attack.

The PCSC also helps to educate children on their vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyberstalking, cyber harassment, cyberbullying or trolling for a target to sexually victimize. In addition to an educational tool, the PCSC has been designed to allow parents, teachers, educators and pediatric professionals to interview, collect data and engage in a dialogue with children about their online practices.

The PCSC combines common factors causing children to be cyberbullied, harassed and targeted by online sexual predators. Based on a parent's internet safety familial endeavors, the PCSC can also be used along with their child and the entire family during family discussions on cyber security.

PCSC CHECKLIST DIRECTIONS

1. The time required to finish the PCSC 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.

PCSC

Parent Cyber Safety Checklist

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__
Assessment 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. A teacher, you or a trusted adult regularly discusses cyberbullying with your child.
2. Your child has not returned home with missing or damaged belongings related to their online activities.
3. Your child knows to ignore being harassed or teased online.
4. Your child has not been flamed (a provoking message) online.
5. Your child has not been harassed or teased online about their race or sexual orientation.
6. Your child has not been threatened, embarrassed or teased online about their physical attributes.
7. Your child has not been negative about school and/or their home environment related to their online activities.
8. Other children have not sent or posted mean messages about your child online.
9. Your child has not been teased or embarrassed online by someone your child, you or teacher does not know.
10. Your child has not had an online relationship involving an adversarial and/or negative outcome.
11. Your child has not had secrets they have disclosed been spread by others online.
12. Other children have not captured, saved or stored embarrassing online information about your child.
13. Your child has not retaliated to online information being spread about them.
14. Your child has not been repeatedly harassed or berated by others online.
15. Your child knows how to respond if a friend is being cyber bullied.
16. Your child knows who, when and how to report a cyber bully.
17. Your child has not received unwanted offensive online content.
18. Your child has not been sexually teased or taunted online.
19. Your child has not been aggressive and/or mean to others online.

20. Your child would not be a bystander if their friend were being cyber harassed and teased.
21. Your child knows what encourages a cyber bully.
22. Your child does not appear sullen going to or returning from school due to their online activities.
23. Your child knows images they post or share online can be used to embarrass them.
24. Your child practices digital citizenship (online manners.)
25. Your child knows what to do if others online are taunting them.
26. Your child has not received offensive information or images online.
27. In the last 90 days, other children have not repeatedly teased your child online.
28. In the last 90 days, other children have not repeatedly lied to your child online.
29. In the last 90 days, your child has not been bullied and/or cyber bullied.
30. In the last 90 days, other children have not repeatedly harassed your child online.

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 children have not posted embarrassing information about your child.
32. Your child is cautious when posting personal information online.
33. Your child knows what "digital footprint" means.
34. Your child has not shared confidential information to a now ex-friend or ex-intimate partner online.
35. Your child practices caution what they disclose online.
36. Your child knows to protect their images from strangers viewing them online.
37. Your child knows how to sustain and monitor a positive Digital Reputation.
38. Your child knows their images can remain in cyberspace for years.
39. Your child knows information shared online may be impossible to delete.
40. Your child does not have a mobile device with information that is embarrassing.
41. Your child knows sexting can be criminal & also shared with others.
42. Your child knows their personal information posted or shared online can go viral.
43. Your child knows everyone has a Digital Footprint.
44. Your child knows images and videos can be reposted multiple times.
45. Your child knows what information can be harmful to their Digital Reputation.
46. You and your child take steps to ensure their Digital Reputation is accurate.
47. You and your child respectfully monitor what information they post.
48. Your child practices good behavior online and in chat rooms.
49. You and your child enter their personal information into search engines.
50. You and your child respectfully check your child's email and social media profiles.
51. Your child has not engaged in sexting.

52. You or a loved one spends time with your child educating them on their Digital Reputation.
53. Your child knows content they share online can be reposted.
54. Your child knows information shared online can hurt their future.
55. Your child does not share provocative images or details online.
56. Your child does not post personal information to impress others online.
57. Your child has not shared privileged information to an ex-friend or ex-partner online.
58. Your child is careful what they tell others online.
59. Your child knows their images and videos can stay in cyberspace for years.
60. Your child knows information about them online 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 ONLINE BEHAVIORS

61. Your child does not have sexual conversations with someone they met online.
62. Your child has not had a Facebook or social networking account prior to age 13.
63. Your child knows to disclose websites they have visited if requested by you or a trusted adult.
64. Your child has not visited or been exposed to online sex sites.
65. Your child does not use the Internet without supervision or an adult familiar with their online activities.
66. Your child has not received or made phone calls to others you or a trusted adult does not know.
67. Your child does not inform others online when an adult will not be home.
68. Your child has not been contacted by an online stranger.
69. Your child has not met anyone in person they met online.
70. A teacher, parent or a trusted adult has not approached your child and they quickly shut off their computer.
71. Your child does not respond to anyone they do not know in chat rooms.
72. Your child has not accepted a phone call from an adult they met online.
73. Your child does not communicate online with adults you do not know.
74. Your child does not isolate in his or her room while online.
75. Your child does not visit chat rooms without an adult's permission or trained chat room moderator.
76. Your child does not engage in online activity in their room without permission from you or a trusted adult.
77. Your child has not engaged in online activities they have been restricted from.
78. Your child knows to log out if they feel uncomfortable or fearful.
79. Your child does not engage in online activities they would not want an adult to know about.

80. Your child would not meet anyone they met online without you or a trusted adult's permission.
81. Your child knows they are at a higher risk being contacted by online strangers at night.
82. Your child has not met in person someone they met online without you or a trusted adult's knowledge.
83. Your child does not accept free software, ring tones or screen savers from online strangers.
84. Your child does not hesitate with loved ones disclosing who they converse with online.
85. Your child does not have names on their "buddy" or "friend" lists you do not know.
86. Your child does not send personal information to others they do not know.
87. Your child has not discussed sex online with people they have met online.
88. Your child has not text messaged or chatted about sex online with others.
89. Your child has not been contacted by phone from an online stranger.
90. Your child has not met anyone in person they met online without telling an adult.

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. You are confident your child has been adequately educated on iPredators.
92. You and your child are aware the iPredators target children using kindness and understanding.
93. You and your child are aware iPredators use attention, affection and gifts to seduce children.
94. You and your child are aware most iPredators are roughly the same age as your child.
95. Your child knows iPredators create profiles pretending to be their same age.
96. You and your child are aware iPredators are educated in areas that children are most intrigued by.
97. You and your child know the ideal age an iPredator targets is between 11 and 14.
98. Your child knows iPredators encourage others to add them to their "friend" or "buddy" lists.
99. Your child knows peer-to-peer networks can expose adult computer to iPredators.
100. You and your child know the best protection from iPredators are safe online communication and Digital Citizenship.
101. You and your child know how to block sites on computers from being accessed by iPredators.
102. You and your child know iPredators use keywords in their sites popular for children.

103. You are aware many children, aged 8-12, explore pornography sites.
104. Your child knows iPredators will pretend to be minors with fake profiles.
105. You and your child are educated on iPredators and the grooming process.
106. Your child is suspicious of anyone who encourages them to be defiant to authority online.
107. You and your child know iPredators encourage children to keep their contacts secret.
108. You and your child are aware most iPredators will be encouraging, patient and reserved.
109. You and your child are aware iPredators offer children their online accounts to converse.
110. You and your child are aware iPredators embed popular child search terms in their sites.
111. You and your child are aware iPredators consistently tell children they are always available to chat online.
112. You are positive your child does not talk to strangers online.
113. You and your child are educated on "grooming" by iPredators in their quest to exploit children.
114. You and your child know file-sharing sites allow iPredators to access portions of their computer.
115. Your child knows iPredators encourage children to share their images online.
116. Your child knows iPredators encourage children to share private information.
117. Your child knows iPredators are kind and understanding.
118. Your child knows iPredators offer gifts to online users.
119. Your child knows iPredators will try to steal their identity.
120. Your child knows iPredators create profiles pretending to be their age.

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. You restrict your child's mobile devices from late night activity.
122. You and your child know children must be 18 years old to activate their GPS services.
123. You and your child know the potential danger of mobile devices with unlimited text messaging and online access.
124. You know the passwords to your child's mobile devices.
125. You and your child know how to prevent unwanted access to their mobile devices.
126. You know how to track the sending of digital photos from your child's mobile devices.
127. If you have a home WiFi system, you run additional firewalls.
128. You and your child are educated on the dangers of GPS location services.

129. You and/or your child knows GPS location services allows anyone to know their exact location.
130. You and/or your child have contacted your child's mobile device service about adult controls.
131. You and your child spend time learning mobile device safety.
132. You and your child know how to install security on your child's mobile devices.
133. You and your child know about near field communications and mobile devices to make purchases.
134. You know children favor text messaging as their primary means of communicating using their mobile phones.
135. You and your child know how to set up remote lock and wipe features in mobile devices.
136. You and your child know how to install security software on your child's mobile devices.
137. You and your child regularly monitor the stored images on their mobile devices.
138. Your child or you have downloaded and installed antivirus software on your child's mobile devices.
139. Your child knows to treat their mobile devices as carefully as their wallets.
140. You or a loved one discourages your child from sharing confidential information with their mobile devices.
141. Your child knows to silence their mobile devices in public places.
142. You set age-appropriate restrictions on your child's mobile Internet usage.
143. Your child complies with school policies regarding mobile device usage.
144. You and your child are aware there are few methods of filtering web content on mobile devices.
145. You are aware that pornographic content is more accessible on mobile devices.
146. You and your child are aware a new trend for children is sexting using their mobile devices.
147. Your child gives their mobile phone passwords to you or a trusted adult.
148. Your child knows how to prevent access to their mobile phone.
149. Your child has learned about the dangers of GPS location services.
150. Your child 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. You are aware peers will introduce to your child questionable web sites.
152. Your child knows to never share his or her password with close friends.
153. You know there is no filtering software that can replace adult supervision.

154. You and your child know they may accidentally disclose his or her phone number by Caller ID.
155. You and your child know it is beneficial for your child to have multiple passwords.
156. You are aware your child has access to their friend's computers and mobile devices.
157. You or a loved one discourages your child from entering private chat rooms.
158. You are aware your child may be exposed to sites dealing with hatred.
159. You or a loved one discourages your child from activating their geolocation services.
160. You and your child are familiar with bot software, spyware, keystroke loggers and viruses.
161. You and your child know that online gaming systems provide extensive communication features.
162. You are prepared for your child visiting adult content websites.
163. You and your child are aware there is technology to identify people your child interacts with.
164. You and your child know how to set a computer's security settings on high.
165. You and your child are familiar with home wireless networks (WiFi) and their security settings.
166. Your child does not participate in online activities an adult does not approve of.
167. You and your child know Facebook is the fastest growing site driven by tweens and teens.
168. Your child knows to never click a link in an unknown email or instant message.
169. You and your child can define unintentional vs. intentional access to offensive online content.
170. Your child does not click on the links in the video comments section.
171. You and your child are aware web sites use keywords from the top twenty brand names for children.
172. You know how to install filters and security software making offensive chat rooms inaccessible.
173. You and your child know how to disable the preview function in your child's email.
174. You and your child know parental control software helps limit the sites your child can access.
175. You and your child have installed the appropriate security controls on your child's mobile devices.
176. You and your child are aware adult websites format their content, so children will view it.
177. You and your child know there is no filtering software that can replace adult supervision.
178. You are aware your child has access to their friend computers and mobile devices.
179. You and your child know that online gaming systems provide extensive communication features.

180. You or your child 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. Your child does not post their home or cell phone numbers on sites without adult permission.
182. Your child knows to be cautious sharing their contact information on gaming sites.
183. Your child does not exchange images from someone they met online.
184. Your child knows to always log off when not using instant messaging.
185. You or a loved one educates your child about the dangers of disclosing their personal information.
186. You and your child confirmed your child's school website is password protected.
187. Your child is cautious posting their email address to prevent screen scrapers.
188. Your child does not post their school name online without adult permission.
189. You or a loved one educates your child about the dangers of sharing personal information online.
190. You encourage your child to be cautious sharing their personal information.
191. Your child's user account names do not include their full or partial real name.
192. Your child does not post their full name or address online without an adult's knowledge.
193. Your child knows how to hide displaying their ID or personal information online.
194. Your child does not post their email address on sites without an adult's permission.
195. Your child does not use text messaging to communicate with others you or teacher does not know.
196. Your child does not disclose their contact information to unknown online contacts.
197. Your child posts other images when prompted to post their own image.
198. Your child does not post their full name, home address or telephone number online.
199. Your child uses various email addresses for different purposes.
200. Your child's email accounts have the highest level of spam filtering is activated.
201. Your child does not post their home address on sites without your permission.
202. Your child does not post their image on sites without adult permission.
203. Your child does not post their personal information without concern or caution.
204. You or a loved one educates your child on being cautious sharing their contact information.

205. Your child does not include their contact information in their profiles or comments.
206. You monitor who your child allows to have their contact information online.
207. Your child knows how posting personal information online can hurt their reputation.
208. Your child has not shared private information to a now ex-friend or ex-partner online.
209. Your child is careful what they tell others online.
210. Your child knows to protect their images from 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. You and your child know how to check your child's Internet history.
212. Your child knows to consult a trusted adult if exposed to graphic content.
213. You or a loved one discourages your child from being a bystander to cyber bullying.
214. You and your child know how to deactivate your child's Caller ID services.
215. You and your child know to contact the police if your child is sexually solicited online.
216. You set rules for your child's online activity inside and outside the home.
217. You and your child are familiar with common chat room lingo used by children.
218. You and your child know what computer safeguards your child's friends have in their homes.
219. Your child's instant messaging contacts and buddy lists are discussed regularly.
220. You monitor pornographic content on your child's internet enabled devices.
221. Your child has daily time limits for being online.
222. You have blocked access from your child visiting adult oriented web sites.
223. You know to prohibit your child from online activity at night unless supervised.
224. You know to monitor your child's "buddy" or "friend" lists on their social sites.
225. You and your child engage in discussions about their friend's online habits.
226. You encourage your child to tell an adult if they receive a sexual solicitation.
227. You remind your child to only download legal files, music and videos.
228. You and your child know how to respond if your child explores sexual websites.
229. You and your child have the appropriate contacts if someone suspicious contacts your child.
230. The friend's parents or adults supervising your child, when they visit friends, have online rules.
231. You discuss with your child possible online dangerous scenarios.
232. You know how to check your child's history folder if they become suspicious.
233. You confirm a trained moderator always monitors chat rooms your child visits.
234. You limit your child's online chatting on their favorite gaming or club sites.

235. Your child knows you or a trusted adult visits some, if not all, sites they frequently visit.
236. You keep all ICT in a communal area of the home that is central to their view.
237. You and your child know to contact the police if your child reports being sexually solicited online.
238. You know sets rules for your child's online activity inside and outside the home.
239. Your child's instant messaging contacts, "friend" and "buddy" lists are checked regularly.
240. You monitor your child's "buddy" or "friend" lists and encourages adult confirmation first.

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. Your child spends more time with friends and less time online.
242. Your child knows it is healthy to have an online curfew.
243. Your child knows to report to a trusted adult if he or she feels unattractive or not liked related to their online activities.
244. Your child knows to report to a trusted adult if he or she feels sad or depressed related to their online activities.
245. Your child posts comments typical of their age online.
246. Your child has not withdrawn from his or her favorite hobbies due to their online activities.
247. Your child does not engage in risk-taking and/or self-destructive behaviors online.
248. Your child has not had a drastic change in grades due to their online activities.
249. Your child has not been less attentive or falling behind in school due to their online activities.
250. Your child's behavior at home and/or school has not changed related to their online activities.
251. Your child does not seem distressed or anxious related to their online activities.
252. Your child does not have little adult involvement due to their online activities.
253. Your child has not reported a loss of appetite or lack of sleep related to their online activities.
254. Your child has not withdrawn from friends and family members related to their online activities.
255. Your child does not have few offline friends and prefers online contacts.
256. Your child does not complain about feeling afraid related to their online activities.
257. You or a teacher does not define your child as being defiant and/or oppositional related to their online activities.

258. Your child has not witnessed a traumatic event or significant adult conflict and shared this information online.
259. Your child has not reported disliking school, the teachers or your children related to their online activities.
260. Your child does not report feeling unaccepted by his/her peers related to their online activities.
261. Your child knows to report to you or a teacher if they feel more accepted by an online adult than their peers or loved ones.
262. Your child does not appear hopeless and/or discouraged related to their online activities.
263. Your child does not become easily upset after using their ICT.
264. Your child does not spend more time online appearing uninterested in family functions or school activities.
265. Your child does not become easily agitated and/or externalizes blame related to their online activities.
266. Your child's friends do not have behavioral/emotional problems in school related to their online activities.
267. Your child has not had a drastic change in grades related to their online activities.
268. Your child does not have little family involvement due to their online activities.
269. Your child has not reported a loss of appetite or lack of sleep related to their online activities.
270. Your child does not complain about stomachaches or feeling ill related 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. Your child does not spend large periods of time online involved with social media.
272. Your child knows to end contact if someone starts asking sexual questions.
273. Your child does not have a social media account that a parent does not inspect.
274. Your child does not have a social media profile with information available to the public.
275. Your child does not share with others his/her social media profile passwords.
276. You and your child know the age restrictions of your child's favorite social media sites.
277. Your child does not visit chat rooms without adult moderation.
278. Your child knows to be cautious of flattering messages received online.
279. Your child knows to keep their social profile pages "*friends only*" for inviting friends or loved ones.

280. You or a loved one spends time educating your child on proper online etiquette.
281. You or a loved one monitors and/or inquiries about the social media sites your child frequents.
282. You have joined and become a "*friend*" or "*buddy*" on your child's social profiles.
283. Your child does not have a mobile device with an application for their social media profile that they habitually use throughout the day.
284. Your child is cautious of who can view photos and videos on their social profile page.
285. You and your child are aware that many social media platforms require a child to be 13 years old to join.
286. You and your child review privacy and security settings on social media sites with your child.
287. Your child knows social media, when used carelessly, is dangerous.
288. You know to prohibit your child from posting their images at a public profile.
289. Your child does not have a social media account you or a trusted adult does not monitor.
290. Your child refrains from allowing others they do not know to join their "friend" or "buddy" lists.
291. Your child does not have any social media profiles set to "Public".
292. Your child knows to refuse "friend" or "buddy" list requests from others they do not know that have been introduced to them by other friends.
293. Your child refrains from responding to strange email messages or IMs from their social media accounts.
294. Your child is respectful online and shares positive information when prompted.
295. Your child is aware people they meet online may lie about their identity.
296. Your child practices caution with their social profiles.
297. Your child knows to end contact if someone starts asking them questions about sex and/or violence.
298. Your child knows to be cautious of flattering messages from others they meet online.
299. You spend time educating your child on proper online etiquette.
300. You and your child have a general understanding of "*Social Media Safety*".

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. Your child does not give out their telephone number to online strangers.
302. Your child knows what to do they receive harassing, slandering or unwanted online message.

303. Your child knows some cyberstalkers impersonate their victim to target and attack others online.
304. Your child knows what to do if they receive unwanted emails or text messages from an ex-partner, acquaintance or stranger.
305. Your child knows what to do they receive unsolicited threatening emails and/or death threats.
306. Your child knows what to do they receive electronic viruses from an ex-partner, acquaintance or stranger.
307. Your child knows what to do they receive spam from an ex-partner, acquaintance or stranger.
308. Your child knows what to do if they are sexually harassed via online posts, emails, mobile device or text messages.
309. Your child knows what to do if cyber harassed, slandered or cyberbullied in chat rooms or forum posts.
310. Your child knows what to do if they find their personal or financial information online posted by an ex-partner, acquaintance or stranger.
311. Your child knows what to do if subscribed to pornography and/or distasteful advertising without their consent.
312. Your child knows to regularly check their computers, cell phones or mobile devices for spyware.
313. You or a loved one checks your child's mobile devices to assess if they are being tracked by GPS technology.
314. You or a loved one checks your child's phone calls or messages to make sure they are not being intercepted.
315. Your child knows what to do if they are being impersonated online.
316. Your child knows if they are cyberstalked, slandered or harassed, there is a good chance it is an ex-partner, acquaintance or peer.
317. Your child knows cyberstalkers contact the victim or target's family, employer, school and financial institution.
318. Your child knows online users who post personal information, when blogging, have higher rates of cyberstalking and harassment.
319. Your child knows cyberstalkers and harassers follow their target from site to site.
320. Your child knows to make sure their email addresses, instant messaging usernames and links to personal homepages cannot be connected to them.
321. Your child knows online users are particularly susceptible to cyberstalking, slander and harassment if video blogging (vlogging).
322. Your child knows a cyberstalker can be an obsessed love interest or someone with a grudge due to a minor or imagined reason.
323. Your child knows cyberstalkers inconspicuously pose as friends or coworkers asking innocuous questions they will use to attempt recovering their target's passwords.
324. Your child has a general understanding of "*Internet Trolls*".
325. Your child knows that cyberstalking can occur whether the offender resides in the same geographic location.

326. Your child knows a cyberstalker can be an egotistic aggressor who wants to show-off to their online peers and/or classmates.
327. Your child knows to avoid announcing their physical location via status updates on GPS-enabled applications.
328. You and your child know changing Internet Service Providers and reporting hostile and/or aggressive events helps to stop cyberstalking.
329. You and your child know it is recommended to contact the local FBI Computer Crimes Unit if habitually threatened with physical harm.
330. Your child knows to never leave a logged in computer unattended.

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__ = PCSC Score__

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

Michael Nuccitelli, Psy.D.
NYS Licensed Psychologist & iPredator Construct Author
iPredator Inc. New York, USA
347-871-2416 info@ipredatorinc.com
www.ipredator.co

PCSC

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 PCSC 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 ICT users are very real and can range from frustrating to deadly". Michael Nuccitelli, Psy.D. (2014)

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 ICT 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

Parent Cyber Safety Checklist
PCSC

Note: Just as all the IISC tools, it is recommended to take the PCSC 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 and cyber criminology consultant. He completed his doctoral degree in clinical psychology from Adler University in 1994. In 2010, Dr. Nuccitelli published his dark side of cyberspace concept called "iPredator." In November 2011, he established iPredator Inc., offering educational, investigative, and advisory services involving online assailants, cyber-attack targets, dark psychology and internet safety. Dr. Nuccitelli has worked in the mental health field over the last thirty-plus years and he has volunteered his time helping cyber-attacked victims since 2010. His goal is to reduce victimization, theft, and disparagement from iPredators.

In addition to aiding citizens & disseminating educational content, Dr. Nuccitelli's mission is to implement a permanent national educational and awareness online safety campaign with the help of private, state, and federal agencies. He is always available, at no cost, to interact with online users, professionals, and the media. To invite Dr. Nuccitelli to conduct training, media engagements, educational services, or consultation, please call him at (347) 871-2416 or via email at drnucc@ipredatorinc.com.

- LinkedIn: Michael Nuccitelli, Psy.D.
- Twitter: @TheiPredator
- Facebook Page: The iPredator
- Facebook: Michael Nuccitelli
- Pinterest: iPredator
- Tumblr: iPredator
- Instagram: #drnucc