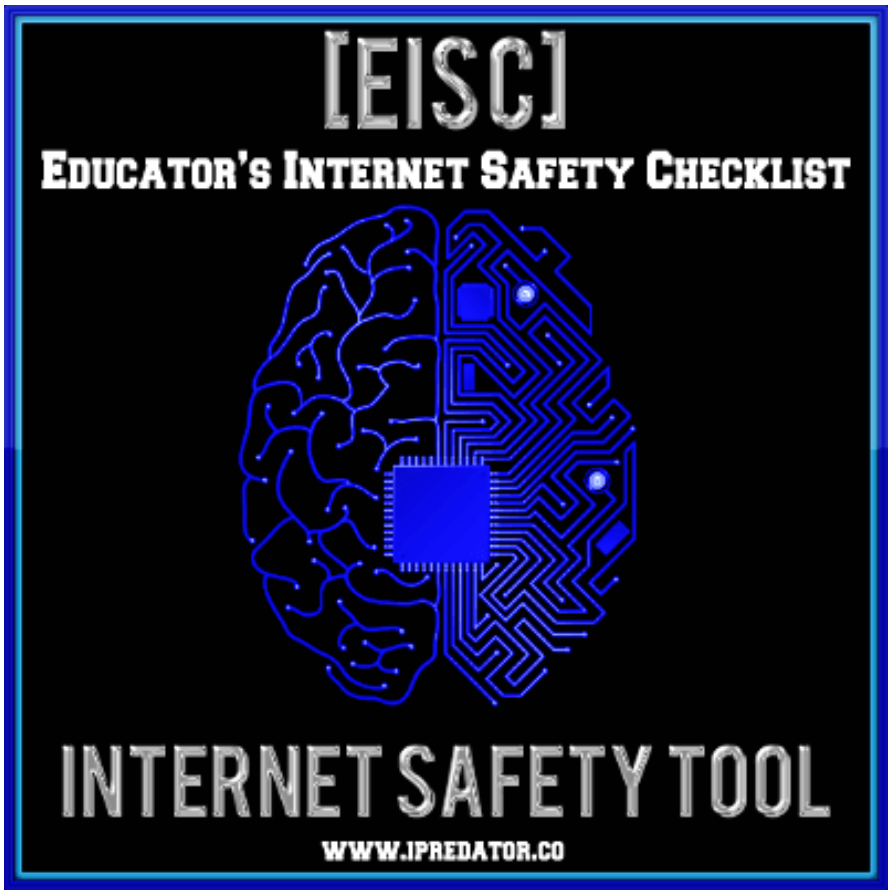
EISC

Educator Internet Safety Checklist

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



Educator Internet Safety Checklist (EISC)

The Educator Internet Safety Checklist is a 330-item data collection, diagnostic and informational tool for educators regarding a student's preparedness and prevention of being cyberbullied, cyber harassed, cyber stalked, sexually solicited and/or victimized by iPredators. In addition to a data collection tool and general educational template, the EISC can also be used as an adjunct to classroom projects, prevention education plans and educator training seminars on internet safety.

The goal of the EISC is to educate children on their vulnerability and risk potential of being targeted by an iPredator that is engaged in cybercrime, cyberstalking, internet trolling, cyber harassment, cyberbullying or online deception. In addition to an educational tool, the EISC has been designed to allow teachers, educators and pediatric professionals to interview, collect data and engage in a dialogue with children about their online practices.

EISC DIRECTIONS

Educator Internet Safety Checklists (EISC)

1. The time required to finish the EISC 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.

EISC

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

21. The student knows what encourages a cyberbully.
22. The student does not appear sullen going to or returning from school due to their online activities.
23. The student knows images they post or share online can be used to embarrass them.
24. The student knows to practice good "*Digital Citizenship*".
25. The student knows what to do if others are taunting them online.
26. The student has not received offensive sexually themed information or images online.
27. In the last 90 days, other students have not repeatedly teased them online.
28. In the last 90 days, other students have not repeatedly lied to them online.
29. In the last 90 days, the student has not been bullied and/or cyberbullied.
30. In the last 90 days, other students have not repeatedly harassed them 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 students have not made false allegations about the student online.
32. The student is cautious when posting personal information online.
33. The student knows what "*Digital Footprint*" means.
34. The student has not shared confidential information to a now ex-friend or ex-intimate partner online.
35. The student knows to practice caution what they disclose online.
36. The student knows to protect their images from strangers viewing them online.
37. The student knows how to sustain and monitor a positive "*Digital Reputation*".
38. The student knows their images can remain in cyberspace for years.
39. The student knows information shared online may be impossible to delete.
40. The student does not have a mobile device with information that is embarrassing.
41. The student knows sexting can be criminal and shared with many others.
42. The student knows their personal information, posted or shared online, can go viral.
43. The student knows everyone has a "*Digital Footprint*".
44. The student knows images and videos can be reposted multiple times.
45. The student knows what information can be harmful to their "*Digital Reputation*".
46. The student and parents take steps to ensure the student's "*Digital Reputation*" is accurate.
47. The student and parents respectfully monitor what information the student posts.
48. The student knows to practice good behavior online and in chat rooms.
49. The student and parents enter the student's personal information into search engines.
50. The student and parents respectfully check the student's email and social media profiles.
51. The student has not engaged in "*Sexting*" or has been the victim of "*Sexting*".
52. The parents or a teacher spends time with the student educating them on their "*Digital Reputation*".

53. The student knows content they share online can be reposted.
54. The student knows information shared online can hurt their future.
55. The student does not share provocative images or details online.
56. The student does not post personal information to impress others online.
57. The student has not shared confidential information to an ex-friend or ex-partner online.
58. The student is careful what they tell others online.
59. The student knows their images and videos can stay in cyberspace for years.
60. The student knows negative 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 ICT

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

80. The student would not meet anyone they met online without the parents or a trusted adult's permission.
81. The student knows they are at a higher risk being contacted by online strangers at night.
82. The student has not met in person someone they met online without the parents or a trusted adult's knowledge.
83. The student does not accept free software, ring tones or screen savers from online strangers.
84. The student does not hesitate with loved ones disclosing whom they converse with online.
85. The student does not have names on their "buddy" or "friend" lists unknown to parents or a trusted adult.
86. The student does not send personal information to others they do not know.
87. The student has not discussed sex online with people they have met online.
88. The student has not text messaged or chatted about sex with online strangers.
89. The student has not been contacted by phone from an online stranger.
90. The student has not met anyone in person he or she 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. The parents are confident the student has been educated on iPredators.
92. The student and/or the parents are aware iPredators target children using kindness and understanding.
93. The student and/or the parents are aware iPredators use attention, affection and gifts to seduce children.
94. The student and/or the parents are aware most iPredators are the same age as the student.
95. The student knows iPredators create profiles pretending to be their same age.
96. The student and/or the parents are aware iPredators are educated in areas that intrigue children.
97. The student and parents know the ideal age an iPredator targets is 11-14 years old.
98. The student knows iPredators encourage others to add them to their "friend" or "buddy" lists.
99. The student knows peer-to-peer networks can expose adult computer to iPredators.
100. The student and parents know the best protection from iPredators is safe online communication and Digital Citizenship.
101. The student and parents know how to block sites on computers from being accessed by iPredators.
102. The student and parents know iPredators use keywords in their sites popular for children.

103. The student and/or the parents are aware many children, aged 8-12, explore sex sites.
104. The student knows iPredators will pretend to be children and teens with fake profiles.
105. The student and parents are educated on iPredators and the grooming process.
106. The student is suspicious of anyone who encourages them to be defiant to authority online.
107. The student and parents know iPredators encourage children to keep their contacts secret.
108. The student and parents are aware most iPredators will be encouraging, patient and reserved.
109. The student and parents are aware iPredators offer children their online accounts to converse.
110. The student and parents are aware iPredators embed popular child search terms in their sites.
111. The student and parents are aware iPredators consistently tell children they are always available to chat online.
112. The parents are positive the student does not talk to strangers online.
113. The student and parents are educated on "grooming" by iPredators in their quest to exploit children.
114. The student and parents know file-sharing sites allow iPredators to access portions of their computer.
115. The student knows iPredators encourage children to share their images online.
116. The student knows iPredators encourage children to share confidential information.
117. The student knows iPredators are kind and understanding.
118. The student knows iPredators offer gifts to online users.
119. The student knows iPredators will try to steal their identity.
120. The student 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. The parents or a trusted adult restricts the students' mobile devices from late night activity.
122. The student and parents know children must be 18 years old to activate their GPS services.
123. The student and parents know the potential danger of mobile devices with unlimited text messaging and online access.
124. The parents or a trusted adult knows the passwords to the students' mobile devices.
125. The student and parents know how to prevent unwanted access to the child's mobile devices.
126. The parents or a trusted adult knows how to track the sending of digital photos from the students' mobile devices.

127. If the parents have a home WiFi system, they run additional firewalls.
128. The student and parents are educated on the dangers of GPS location services.
129. The student and parents know GPS location services allow anyone to know their exact location.
130. The student or the parents have contacted the student's mobile device service about adult controls.
131. The student and parents spend time learning mobile device safety.
132. The student, the parents or a trusted adult knows how to install security on the students' mobile devices.
133. The student, the parents or a trusted adult knows about near field communications and mobile devices to make purchases.
134. The parents know children favor text messaging as their primary means of communicating using their mobile phones.
135. The student and parents know how to set up remote lock and wipe features in mobile devices.
136. The student and parents know how to install security software on the students' mobile devices.
137. The student and parents regularly monitor the stored images on their mobile devices.
138. The student or the parents have downloaded and installed antivirus software on the students' mobile devices.
139. The student knows to treat their mobile devices as carefully as their wallets.
140. The parents or teacher discourages the student from sharing private information with their mobile devices.
141. The student knows to silence their mobile devices in public places.
142. The parents set age-appropriate restrictions on the student's mobile Internet usage.
143. The student complies with school policies regarding mobile device usage.
144. The student and parents are aware there are few methods of filtering web content on mobile devices.
145. The parents are aware that pornographic content is more accessible on mobile devices.
146. The student and parents are aware a new trend for children is sexting using their mobile devices.
147. The student gives their mobile phone passwords to the parents or a trusted adult.
148. The student knows how to prevent access to their mobile phone.
149. The student has learned about the dangers of GPS location services.
150. The student 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 parents or a trusted adult is aware the student will be introduced by peers to questionable web sites.
152. The student knows to never share his or her password with close friends.
153. The parents or a trusted adult knows there is no filtering software that can replace adult supervision.
154. The student and parents know the student may accidentally disclose his or her phone number by Caller ID.
155. The student and parents know it is beneficial for the student to have multiple passwords.
156. The parents or a trusted adult is aware the student has access to their friends' computers and mobile devices.
157. The parents or teacher discourages the student from entering private chatrooms.
158. The parents or a trusted adult is aware the student may be exposed to sites dealing with hatred.
159. The parents or teacher discourages the student from activating their geolocation services.
160. The student and parents are familiar with bot software, spyware, keystroke loggers and viruses
161. The student and parents know that online gaming systems provide extensive communication features.
162. The parents are prepared for the student visiting adult content websites.
163. The student and parents are aware there is technology to identify people the student interacts with without their consent.
164. The student and parents know how to set a computer's security settings on high.
165. The student and parents are familiar with home wireless networks (WiFi) and their security settings.
166. The student does not participate in online activities an adult does not approve of.
167. The student and parents know Facebook is the fastest growing site driven by tweens and teens.
168. The student knows to never click a link in an unknown email or instant message.
169. The student and parents can define unintentional vs. intentional access to offensive online content.
170. The student does not click on links in the video comments section.
171. The student and parents are aware web sites use keywords from the top twenty brand names for children.
172. The parents or a trusted adult knows how to install filters and security software making offensive chat rooms inaccessible.
173. The student and parents know how to disable the preview function in the student's email.
174. The student and parents know parental control software helps limit the sites the student can access.
175. The student or the parents have installed the appropriate security controls on the students' mobile devices.

176. The student and parents are aware adult websites format their sites, so children will view it.
177. The student and parents know there is no filtering software that can replace adult supervision.
178. The parents or a trusted adult is aware the student has access to their friends' computers and mobile devices.
179. The student and parents know that online gaming systems provide extensive communication features.
180. The parents or student 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 student does not post their home or cell phone numbers on sites without adult permission.
182. The student knows to be cautious sharing their contact information on gaming sites.
183. The student does not exchange images from someone they met online.
184. The student knows to always log off when not using instant messaging.
185. The parents or teacher educates the student on the dangers of disclosing their personal information.
186. The student and parents confirmed the student's school website is password protected.
187. The student is cautious posting their email address to prevent screen scrapers.
188. The student does not post their school name online without adult permission.
189. The parents or teacher educates the student on the dangers of sharing personal information online.
190. The parents or teacher encourages the student to be cautious sharing their personal information.
191. The student's user account names do not include their full or partial real name.
192. The student does not post their full name or address online without an adult's knowledge.
193. The student knows how to hide displaying their ID or personal information online.
194. The student does not share their email address in anonymous chat or video sites.
195. The student does not use text messaging to communicate with others the parents or teacher does not know.
196. The student does not disclose their contact information to unknown online contacts.
197. The student posts other images when prompted to post their own image.
198. The student does not post their full name, home address or telephone number online.
199. The student uses various email addresses for different purposes.
200. The student's email accounts have the highest level of spam filtering activated.
201. The student does not post their home address on sites without adult permission.

202. The student does not post their image on sites without adult permission.
203. The student does not post or shares their personal information without concern or caution.
204. The parents or teacher educates the student on being cautious sharing their contact information.
205. The student does not include their contact information in their profiles or comments.
206. The parents or a trusted adult monitors who the student allows to have their contact information online.
207. The student knows how posting personal information online can hurt their reputation.
208. The student has not shared confidential information to a now ex-friend or ex-partner online.
209. The student is careful what they disclose to others online.
210. The student 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. The student and parents know how to check the student's Internet history.
212. The student knows to consult a trusted adult if exposed to graphic content.
213. The parents or teacher discourages the student from being a bystander to cyber bullying.
214. The student and parents know how to deactivate the student's Caller ID services.
215. The student and parents know to contact the police if the student is sexually solicited online.
216. The parents set rules inside and outside the home for the student's online activity.
217. The student and parents are familiar with common chat room lingo used by children.
218. The student and parents know what computer safeguards the student's friends have in their homes.
219. The student's instant messaging contacts and buddy lists are discussed regularly.
220. The parents or a trusted adult knows to monitor pornographic content on the student's computer.
221. The student has daily time limits for being online.
222. The parents or a trusted adult has blocked access from the student visiting adult oriented web sites.
223. The parents or a trusted adult knows to prohibit the student from online activity at night unless supervised.
224. The parents or a trusted adult knows to monitor the student's "buddy" or "friend" lists on their social sites.
225. The student and parents engage in discussions about their friends' online habits.
226. The parents encourage the student to tell an adult if they receive a sexual solicitation.
227. The parents remind the student to only download legal files, music and videos.

228. The parents or a trusted adult know how to respond if the student explores sexual websites.
229. The student and parents have the appropriate contacts if the student is contacted by someone suspicious.
230. The parents or adults supervising the student, when they visit friends, have online rules.
231. The parents discuss with the student possible online dangerous scenarios.
232. The parents or a trusted adult knows how to check the student's history folder if they become suspicious.
233. The parents or a trusted adult confirms chat rooms the student visits are always monitored by a trained moderator.
234. The parents or a trusted adult knows to limit the student's online chatting on their favorite gaming or club sites.
235. The student knows the parents or a trusted adult visits some, if not all, sites they frequently visit.
236. The parents or a trusted adult keeps all ICT in a communal area of the home that is central to their view.
237. The student and parents know to contact the police if the student reports being sexually solicited online.
238. The parents or a trusted adult sets rules for the student's time spent in chatrooms.
239. The student's instant messaging contacts, "friend" and "buddy" lists are checked regularly.
240. The parents or a trusted adult monitors the student'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. The student spends more time with friends and less time online.
242. The student knows it is healthy to have an online curfew.
243. The student knows to report to a trusted adult if he or she feels unattractive or unliked related to their online activities.
244. The student knows to report to a trusted adult if he or she feels sad or depressed related to their online activities.
245. The student posts comments typical of his/her age and maturity level online.
246. The student has not withdrawn from his or her favorite hobbies related to their online activities.
247. The student does not engage in risk-taking and/or self-destructive behaviors online.
248. The student has not had a drastic change in grades due to their online activities.
249. The student has not been less attentive or falling behind in school due to their online activities.

250. The student's behavior at home and/or school has not changed related to their online activities.
251. The student does not seem distressed or anxious related to their online activities.
252. The student does not have little adult involvement due to their online activities.
253. The student has not reported a loss of appetite or lack of sleep related to their online activities.
254. The student has not withdrawn from friends and family members related to their online activities.
255. The student does not have few offline friends and prefers online contacts.
266. The student does not complain about feeling afraid related to their online activities.
257. The parents or a teacher does not define the student as being defiant and/or oppositional related to their online activities.
258. The student has not witnessed a traumatic event or significant adult conflict and shared this information online.
259. The student has not reported disliking school, the teachers or the students related to their online activities.
260. The student does not report feeling unaccepted by his/her peers related to their online activities.
261. The student knows to report to the parents or teacher if they feel more accepted by an online adult than their peers or loved ones.
262. The student does not appear hopeless and/or discouraged related to their online activities.
263. The student does not become easily upset after using their ICT.
264. The student does not spend more time online appearing uninterested in family functions or school activities.
265. The student does not become easily agitated and/or externalizes blame related to their online activities.
266. The student's friends do not have behavioral/emotional problems in school related to their online activities.
267. The student has not had a drastic change in grades related to their online activities.
268. The student does not have little peer involvement, or none related to their online activities.
269. The student has not reported a loss of appetite or lack of sleep 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

270. The student does not complain about stomachaches or feeling ill related to their online activities.

271. The student does not spend large periods online involved with Facebook and/or other social networking sites that are not academic or career related.
272. The student knows to end contact if someone starts with questions about sex.
273. The student does not have a Facebook and/or other social networking site accounts the parents or a trusted adult rarely visits.
274. The student does not have a social media profile with information available to the public.
275. The student does not share with others his/her social media profile passwords.
276. The student and parents know the age restrictions of the students' favorite social media sites.
277. The student does not visit chatrooms without adult moderation.
278. The student knows to be cautious of flattering messages received online.
279. The student knows to keep their social profile pages "friends only" for inviting friends or loved ones.
280. The parents or teacher spends time educating the student on proper online etiquette.
281. The parents' monitor and/or inquiries about the social media sites the student frequents.
282. The parents or a trusted adult has joined and become a "friend" or "buddy" on the student's social profiles.
283. The student does not have a mobile device with an application for their social media profile that they use habitually throughout the day.
284. The student limits on their profile page who can view his or her images and videos.
285. The student and parents are aware Facebook requires a child to be 13 years old before they can sign up.
286. The student and parents review the privacy and security settings on social media sites with the student.
287. The student knows social media when used carelessly is dangerous.
288. The parents or a trusted adult knows to prohibit the student from posting their images at a public profile.
289. The student does not have a Twitter account the parents or a trusted adult does not monitor.
290. The student refrains from allowing others they do not know to join their "friend" or "buddy" lists.
291. The student does not have their Facebook or social media profiles set to "Friends of Friends" or "Public".
292. The student knows to refuse "friend" or "buddy" list requests from others they do not know that have been introduced to them by other friends.
293. The student refrains from responding to strange email messages or IM's from their social media accounts.
294. The student is respectful online and shares positive information when prompted.
295. The student is aware people they meet online may lie about who they are.
296. The student knows to practice caution with their social profiles.
297. The student is aware anonymous text and online users engaged in nefarious activities frequent video chat sites.
298. The student knows to be cautious of flattering messages from others they meet online.

299. The student and parents spend time discussing proper online etiquette.
300. The parents or a trusted adult has joined and become a "friend" or "buddy" on the student's social profiles.

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. The student does not give out their Social Security Number to unknown online requests.
302. The student knows what to do if they receive harassing, slandering or unwanted communication online.
303. The student knows cyber stalkers impersonate their victim to target and attack others online.
304. The student knows what to do if they receive unwanted emails or text messages from an ex-partner, acquaintance or stranger.
305. The student knows what to do if they receive unsolicited threatening emails and/or death threats.
306. The student knows what to do if they receive electronic viruses from an ex-partner, acquaintance or stranger.
307. The student knows what to do if they receive extreme amounts of spam from an ex-partner, acquaintance or stranger.
308. The student knows what to do if sexually harassed via online posts, emails, phone or text messages.
309. The student knows to tell an adult if cyber harassed, slandered or cyberbullied.
310. The student knows what to do if they find their personal or financial information online posted by an ex-partner, acquaintance or stranger.
311. The student knows what to do if subscribed to pornography and/or distasteful advertising without their consent.
312. The student knows to regularly check their computers, cell phones or mobile devices for spyware.
313. The student, the parents or a trusted adult knows to check if their mobile devices are being tracked by GPS technology.
314. The student, the parents or a trusted adult knows to check if their phone calls or messages are being intercepted.
315. The student knows what to do if being impersonated online.
316. The student knows if being cyber stalked, slandered or harassed, there is a good chance it is an ex-partner, acquaintance or peer.
317. The student knows cyberstalkers contact the victim or target's family, employer, school and financial institution.
318. The student knows online users who post personal information when blogging have higher rates of cyber stalking and harassment.

319. The student knows cyberstalkers and harassers follow their victim or target from site to site.
320. The student knows to make sure their email addresses, instant messaging usernames and links to personal homepages cannot be connected to them.
321. The student knows online users are particularly susceptible to cyber stalking, slander and harassment if video blogging (vlogging.)
322. The student knows a cyber stalker can be an obsessed love interest or someone with a grudge due to a minor or imagined reason.
323. The student knows cyber stalkers inconspicuously pose as friends or coworkers asking innocuous questions they will use to attempt recovering their target's passwords.
324. The student knows that most cyber stalking, Internet slander and harassment involves someone they know or interacted with in the recent past.
325. The student knows that cyber stalking, Internet slander and harassment can occur whether the offender or target resides or works in the same geographic location.
326. The student knows a cyber stalker can be an egotistic aggressor who wants to show-off to their peers, online peers and/or classmates.
327. The student knows to avoid announcing their physical location via status updates of GPS-enabled applications.
328. The student knows changing Internet Service Providers and reporting hostile, and/or aggressive events is recommended to stop cyberstalking and/or internet slander.
329. The student knows to contact the local FBI Computer Crimes Unit if cyberstalked, threatened or harassed by an adult online stranger.
330. The student knows an unattended logged in computer 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__ = EISC 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 EISC 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.

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

Educator Internet Safety Checklist
EISC

Note: Just as all the IISC tools, it is recommended to take the EISC 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.