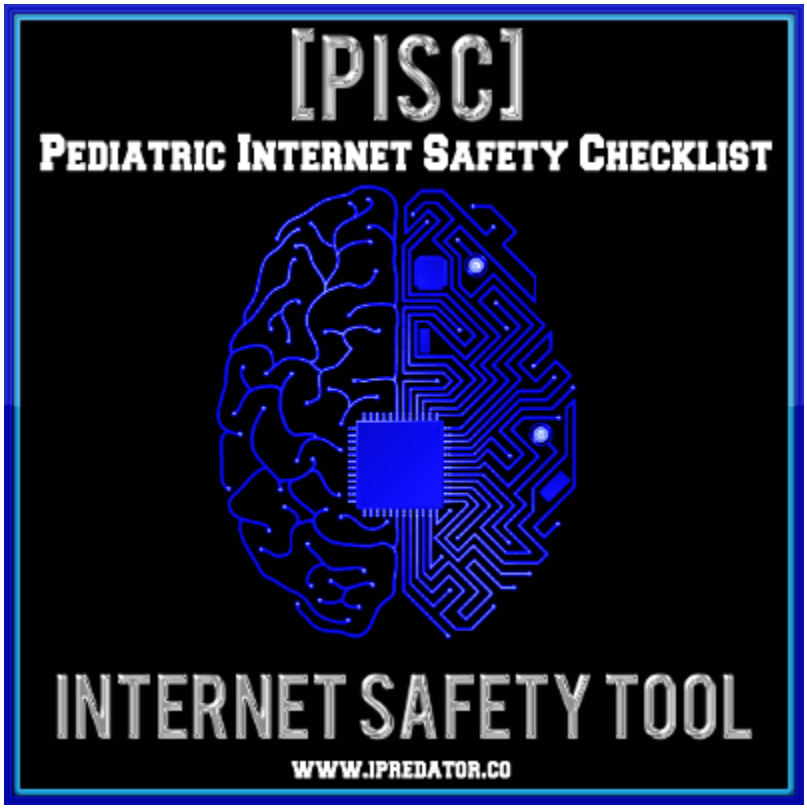
PISC

Pediatric Internet Safety Checklist

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



Pediatric Internet Safety Checklist (PISC)

The Pediatric Internet Safety Checklist is a 100-item education, assessment and data collection tool designed for parents, educators and pediatric professionals on child internet safety and responsible online usage. The PISC queries and explores areas developmentally relevant to an early adolescent, adolescent and young adult, ages 11-21.

The goal of the PISC is to educate children on their vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyberstalking, cyber harassment, cyberbullying or online child predation.

In addition to an educational tool, the PISC 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 PISC combines common factors causing children to be cyber bullied, harassed and targeted by online sexual predators. The PISC also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

PISC DIRECTIONS

1. The time required to complete the PISC checklists averages 60-90 minutes.

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

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

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

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

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

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

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

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

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

iPredator: A child, adult, group or nation who, directly or indirectly, engages in exploitation, victimization, stalking, theft or disparagement of others using Information and Communications Technology (ICT.) iPredators are driven by

deviant fantasies, desires for power and control, retribution, religious fanaticism, political reprisal, psychiatric illness, perceptual distortions, peer acceptance or personal and financial gain. iPredators can be any age, either gender and not bound by economic status, race or national heritage.

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

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

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

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

PISC

Pediatric Internet Safety Checklist

Gender: Male__ Female__

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

Average Daily Online Activity: 0-1Hours__1-3 Hours__3-5 Hours__5+ Hours__

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

1. The child or a trusted adult knows how to install and activate the security features on their mobile device.
2. In the last 90 days, no one has made a racial, sexist, sexual or derogatory statement about the child's family online.
3. In the last 90 days, no one has posted a lie or false allegation about the child online.
4. In the last 90 days, no one has flamed (angry or provocative message) the child.
5. In the last 90 days, the child has not been bullied or cyberbullied.
6. In the last 90 days, no one the child knows has been cyberbullied.
7. The child has not sent, posted or received mean messages about others.
8. In the last 6 months, the child has not had a friend or enemy spread rumors about them.
9. In the last 6 months, the child has not had a friend or enemy disclose a secret about them online.
10. The child knows to never tease or hurt anyone's feelings online.
11. The child knows what to do if they or a friend is cyberbullied.
12. The child's address and phone number are hidden from everyone other than trusted adults.
13. The child knows posting personal information online can hurt their reputation.
14. The child has not shared confidential information to a new ex-friend or ex-romantic partner online.
15. The child is careful what they tell others online, which an adult has verified through discussions or proof.
16. The child protects their images from online strangers viewing them.
17. The child has a positive "*Digital Reputation*".
18. The child knows their images and videos can remain in cyberspace for years.
19. The child knows negative online information about may be impossible to delete.
20. The child does not have a mobile device with information that is embarrassing.
21. The child knows "*Sexting*" may be a criminal act if shared with others.
22. The child has not and would not talk about sex with someone they met online.
23. The child does not have a social profile set to "public" in their privacy settings.

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)

24. The child does not tell friends their passwords.
25. The child has not communicated in chat rooms with online strangers.
26. The child has been educated about the cybercrime called "*Sextortion*".
27. The child has never been contacted by or conversed with an online stranger.
28. The child has never met an online stranger offline without telling a parent or trusted adult.
29. The child has never turned off, logged out or closed their internet enabled device when an adult walked in.
30. The child does not accept online strangers to their "buddy" or "friends" lists.
31. The child does not chat with others they do not know and keep it a secret from an adult.
32. The child has learned about iPredators, online sexual predators and cyberbullying.
33. The child knows iPredators are usually kind and understanding.
34. The child knows iPredators offer gifts to online users.
35. The child knows iPredators will try to steal their identity.
36. The child knows iPredators create profiles pretending to be their age.
37. The child knows to never share online images or videos to online strangers.
38. The child knows peer-to-peer networks (P2P) expose their computer/networks to iPredators.
39. The child knows the best protection from iPredators is being honest and open with their parents & trusted adults.
40. The child has a password or PIN number that locks their mobile device.
41. The child knows to never let an online associate to persuade them to lie to their parents or trusted adults about their online activities
42. The child knows iPredators constantly look for young people online late at night.
43. The child has a mobile device that is password protected in case it is lost or stolen.
44. The child knows how to prevent access to his/her mobile device.
45. The child has learned about the dangers of GPS location services.
46. The child knows GPS location services allow anyone to know their exact location.
47. The child or a trusted adult knows how to install and update their mobile device security filters and controls.
48. The child has learned about "*Mobile Device Safety*".
49. The child is familiar with the two main types of cyberbullying: direct and indirect attacks (aka, cyberbullying by proxy).
50. The child knows and follows his/her school's rules on mobile device usage.
51. Antivirus software is installed on the child's mobile devices.
52. The child and their friends never frequent pornography or dangerous websites.

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)

53. The child knows to never share passwords with loved ones not approved by parents or a trusted adult.
54. The child knows not to post their home or mobile phone numbers online.
55. The child knows they can disclose their phone number by "*Caller ID*" to others they do not know.
56. The child knows it is good to have many passwords they change often.
57. Friends do not know the child's social media account passwords.
58. The child has not and would not visit adult chat rooms and keep it a secret from a parent or trusted adult.
59. The child knows what to do if they are encouraged to visit hate, violence or racist website.
60. The child knows about bot software, spyware, keystroke loggers and viruses.
61. The child knows that social sites are frequented by iPredators.
62. The child does not share their home or mobile phone numbers in chat rooms.
63. The child does not share personal information while online gaming.
64. The child does not share their images or videos with online strangers they consider friends.
65. The child always logs off when not using instant messaging.
66. The child knows about the dangers of sharing their full name online.
67. The child's school website is password protected from online strangers viewing students.
68. The child tells their friends about the dangers of sharing personal information online.
69. The child makes sure social sites they have joined do not show their personal information publicly.
70. None of the child's user account or profile names include their full or partial real name.
71. The child does not post their full name or home address online.
72. The child knows to never give out his or her password to anyone online.
73. The child discourages friends from cyberbullying or teasing others online.
74. The child has rules for their online activities inside and outside the home.
75. The child knows what security software friends have at their homes and/or on their mobile devices.
76. The child knows to tell their parents or a trusted adult if they unintentionally receive pornographic content.
77. The child has daily time limits for being online.
78. The child does not go online at the same time every night.
79. The child knows to tell a parent or a trusted adult if they receive an online sexual message.

80. The child only downloads legal files, music and videos and familiar with "*Digital Piracy*".
81. The child knows to tell a parent or trusted adult if another adult contact them online.
82. The child does not spend less time with friends and family and more time online.
83. The child has an online curfew to shut off their internet enabled devices.
84. The child would talk to a parent, a teacher or trusted adult if they felt unattractive, unpopular, angry or sad.
85. The child would not talk to someone they met online if they felt angry, sad or depressed.
86. The child does not feel more comfortable online than spending time with friends or family offline.
87. The child has not become less interested in their favorite offline activities.
88. The child does not engage in online or offline risk-taking an adult or teacher would say is self-destructive or not healthy.
89. The child has not fallen behind in school from being online too much.
90. A parent, family member or school official has not reported the child's behavior having recently drastically changed.
91. The child knows to speak with a parent, teacher or trusted adult if they feel stressed, anxious or depressed because of conflict at home or school.
92. The child has never been suspected of being internet addicted.
93. The child is not allowed to check their social accounts more than ten times a day.
94. The child does not have a social profile with sexually themed content.
95. The child does not share their private or personal details on a blog or online diary.
96. The child does not visit chat rooms without moderators.
97. The child does not have a social account that a parent or adult does not occasionally monitor.
98. The child does not visit or engage in text or video chats at anonymous chat sites.
99. The child is not overly secretive about his/her online contacts.
100. The child spends an equal time offline as he/she spends 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)

Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Yes Answers__ + Does Not Apply__ = PISC Score__

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

Note: The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. *"I Do Not Know"* & *"No"* responses should be addressed immediately with a plan of action.

(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 PISC 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 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 0-300 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

Pediatric Internet Safety Checklist
PISC

Note: Just as all the IISC tools, it is recommended to take the PISC on a quarterly basis. The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. "IDK" & wrong responses should be addressed immediately with a structured plan of action.

If and/or when you score a 90 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: (1-10)
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: (11-29)
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: (30-39)
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: (40-55)
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: (56-78)
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: (79-89)
Category: Skilled iPredator Protection and Low Vulnerability.
Risk Potential: Mild.
iPredator Involvement: Possible, but Unlikely.
Intervention Plan: Continue iPredator Protection & Prevention Strategies.
Level of Urgency: Not Urgent, Important to Address if Score Below 85.

Score: (90-100)
Category: Advanced iPredator Protection and Minimal Vulnerability.
Risk Potential: Minimal.
iPredator Involvement: Unlikely.
Intervention 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.