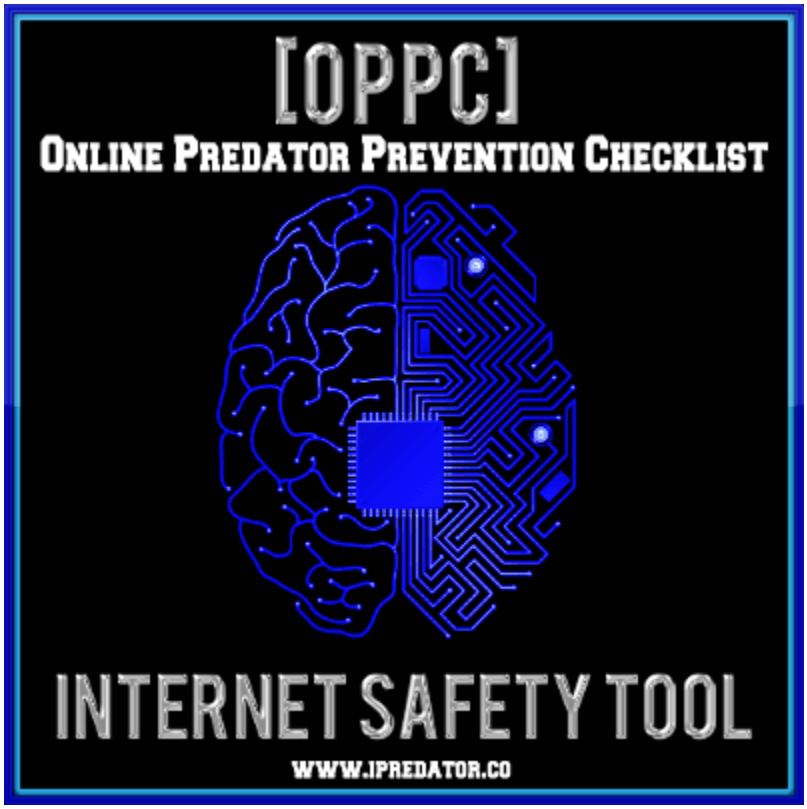
OPPC

Online Predator Prevention Checklist

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



Online Predator Prevention Checklist (OPPC)

The Online Predator Prevention Checklist is a 100-item data collection & educational tool designed to educate and investigate a child, adolescent or young adult's vulnerability and risk potential of being targeted, sexually solicited and/or victimized by online sexual predators. The OPPC investigates areas developmentally relevant to a child and young adult, ages 8-21, which can increase their levels of vulnerability. These areas include sexuality, intimate partnerships, curiosity and motivation for peer group acceptance.

A parent, primary care giver, educator or pediatric professional completes the OPPC. If developmentally appropriate, the OPPC can be completed with the subject child and an adult. In addition to being a data collection & educational tool, the OPPC can also be used as an adjunct to allow teachers, educators and pediatric professionals interview, collect data and engage in a dialogue with children on their online practices.

The OPPC combines common factors causing children to be sexually solicited, harassed and targeted by online sexual predators. The OPPC also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

OPPC CHECKLIST DIRECTIONS

1. The time required to complete the OPPC 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.

Online Predator Prevention Checklist

(OPPC)

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. You know internet sex crimes, involving adults and children, more often fit a model of statutory rape.
2. You use developmentally appropriate prevention strategies to educate the child on romance and sex.
3. You know how to recognize if the child has sexual orientation concerns or patterns of offline and online risk taking.
4. You know the characteristics of internet-initiated sex crimes.
5. You know the stereotype of the iPredator using trickery and violence to assault children is inaccurate.
6. You know most internet sex crimes involve young adult men who seduce underage adolescents into sexual encounters.
7. You know the majority of internet sex crimes involve victims aware they are conversing online with adults.
8. You know iPredators rarely deceive their victims about their sexual interests.
9. You know most children who meet an iPredator face-to-face go to such meetings expecting to engage in sexual activity.
10. The child is aware iPredators primarily deceive children using promises of love and romance, but their intentions are sexual.
11. You know most iPredators are charged with statutory rape involving non-forcible sexual activity with their victims.
12. You know age-of-consent law violations are the most common sex crimes against minors.
13. You know most sex crimes against children are never reported to law enforcement.
14. You know that internet sex crimes, pursued by law enforcement, mostly involves adult offenders who are 10 or more years older than their underage victims.
15. You know the subject child is experiencing or soon to experience adolescent sexual development with growing sexual curiosity.
16. You know most early adolescent children are already aware of, thinking about and beginning to experiment with sex.
17. You know by adolescence, most children have had romantic partners and absorbed by romantic concerns.
18. You know internet sex crimes more often involve self-disclosure and intensity rather than face-to-face relationships.
19. You know children often struggle with emotional control during their early to mid-teens.

20. You know children are vulnerable to grooming due to immaturity, inexperience and the impulsiveness of exploring normal sexual urges.
21. You know children who send personal information to online strangers are more likely to receive sexual solicitations.
22. You know iPredators groom children by establishing trust and confidence first.
23. The child knows to never disclose their personal information at anonymous video chat sites.
24. The child is aware chat rooms are one of the prime arenas iPredators seek out child victims.
25. The child is aware many chat rooms engage in explicit sexual talk, sexual innuendo, and profanity.

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)

26. The child is aware many chat rooms that engage in explicit sexual talk are frequented by adult iPredators.
27. You know that children who habitually visit chat rooms tend to be sad, lonely or depressed.
28. You know that children who habitually visit chat rooms tend to have more problems with parents and engage in risky behavior.
29. You know that children who habitually visit chat rooms tend to be compensating for the obstacles they have forming offline relationships.
30. You know most children are not developmentally prepared to avoid or effectively respond to the sexual invitations online.
31. You know most iPredators meet their child victims in chat rooms.
32. You know children with histories of sexual, physical and emotional abuse are vulnerable to iPredator grooming.
33. You know children with histories of sexual, physical and emotional abuse are far more likely to receive online sexual solicitations.
34. You know emotionally abused children are at risk for online sexual victimization and exploitation.
35. You know children are vulnerable to online sexual solicitations because they are looking for attention and affection.
36. You know childhood trauma is associated with adolescent risk behavior(s), risky sexual behavior(s) and online risk behavior(s).
37. You know prior childhood abuse may trigger risky offline and online sexual behavior(s) that directly invites iPredator advances.
38. You know social skill deficits and depression have been suggested to increase a child's vulnerability to iPredator sexual abuse.
39. You know the only online activity that is riskier than posting online personal information is conversing with online strangers about sex.

40. You know child predators have not changed their tactics due to the growth of social networking sites
41. You know iPredators often stalk children based on the information they share on their social networking profiles
42. You know iPredators rarely target children who they believe are not susceptible to their grooming and seduction tactics.
43. You know children that post their personal information publicly are at a higher risk of being targeted by an iPredator.
44. You know children are more likely to receive online sexual solicitations via instant messages or in chat rooms than through social networking sites.
45. You know that children who have mobile devices that are not monitored by an adult are at a greater risk of being victimized by an iPredator.
46. The child does not post or share contact and/or personal information, images or videos online without an adult's knowledge.
47. The child does not post or share contact and/or personal information online that is provocative, violent, sexually suggestive or age inappropriate.
48. The child does not post or share contact and/or personal information online with adults unknown to the primary caregiver.
49. The child does not post or share contact and/or personal information online with adults unknown to the child.
50. The child does not post or share sexual information online with anyone.

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)

51. The child does not have unknown people on his/her "buddy" or "friends" list.
52. The child does not comment on adult pornography websites.
53. You know that children who interact with online strangers are more likely to receive sexual solicitations.
54. You know that female children and LGBT male children are most likely to receive online sexual solicitations.
55. You know the fundamental differences between a *"Pedophile"* and *"Child Molester"*.
56. You know online sexual solicitations are requests to engage in sexual activities, sexual talk or to share sexual information.
57. You know posting images and videos, involving children, is valued by child predators.
58. You have a general idea on the differences between a "*Child Molester*" & "*Pedophile*".
59. You know the act of violence is rare in online sex crimes.
60. You know iPredators seek to develop relationships with children before they introduce sexual topics.
61. You know iPredators use child pornography to groom and seduce children.

62. The child knows to never send images to online strangers.
63. You know a sexual relationship between an adult and minor is against the law.
64. You are proactive in helping the subject child to feel accepted and loved.
65. You are proactive in focusing on child developmental concerns, including independence, sexuality and romance.
66. You are proactive in focusing on sexual feelings, urges and curiosity that are paramount to a child.
67. When developmentally appropriate, you are prepared to educate the subject child about the dynamics of iPredators and their online tactics.
68. You have or will inform the child that it is normal to have strong sexual feelings, but wrong for adults to exploit those feelings.
69. The child is regularly taught "*Mobile Device Safety*".
70. The child knows the dangers and pitfalls of posting personal information online.
71. The child knows the danger of talking to online strangers with their mobile devices.
72. The child knows the danger of allowing their friends to share their personal information to online strangers.
73. The child knows the danger of using the internet to make rude and hateful comments to both online strangers and known associates.
74. The child knows the danger of sharing personal information to online strangers introduced to them by friends.
75. The child has a strong password on their mobile device.

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)

76. The child knows to never engage in "*Sexting*".
77. The child knows about "*Sextortion*" and that they will never be punished when they tell a parent, loved one or primary caregiver.
78. The child knows to never share or download sexual content involving minors.
79. The child knows what to do if a chat room participant sends them a sexually explicit message.
80. The child knows to never meet an online stranger offline without a parent or primary caregiver present.
81. You know iPredators are drawn to children that appear needy or submissive online.
82. You know iPredators are drawn to children that have their age or birth date in their username.
83. The child has offline friends and not the type to spend all their free time online.
84. You know iPredators seek to isolate children and exploit their emotional vulnerabilities.
85. The child knows to never engage in provocative discussions in anonymous video chat sites.

86. The child knows to never send nude or suggestive pictures using their mobile device.
87. The child knows to turn off their geo location, Bluetooth, and WiFi features, on their mobile devices, when not using them
88. An adult or primary caregiver has role played or will role play with the child various dangerous online scenarios.
89. If the child is given online privacy, they do not engage hi-risk online activities.
90. You or a primary caregiver knows how to adjust the parental controls offered by Internet Service Providers (ISP).
91. You or the child only installs applications from trusted sources and reads the privacy policies.
92. You or the child keeps their mobile device software up to date.
93. The child honestly discloses the websites they regularly visit.
94. The child does not visit, spend money or open emails or attachments from online sex sites.
95. You or the child installs up-to-date virus and malware protection on their mobile device(s).
96. You are positive that the subject child's mobile device is locked by a PIN number or password.
97. The child knows to never tell online contacts when a parent or loved one will not be home.
98. The child knows, in many states, they can be prosecuted for child pornography if they engage in sexting.
99. The child knows to never send or share sexually themed content if they are threatened with "*Sextortion*",
100. The child has never quickly shut off their internet enabled device when a parent or loved walked in their bedroom.

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__ = CCPC 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. Although obtaining a score of 90 or higher indicates a minimal probability of a successful cyber-attack, it is still crucial to be alert and prepared to defend against iPredators, ex-partners and those who would seek to destroy your digital reputation.

(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 OPPC 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 0-300 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

Online Predator Prevention Checklist
OPPC

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