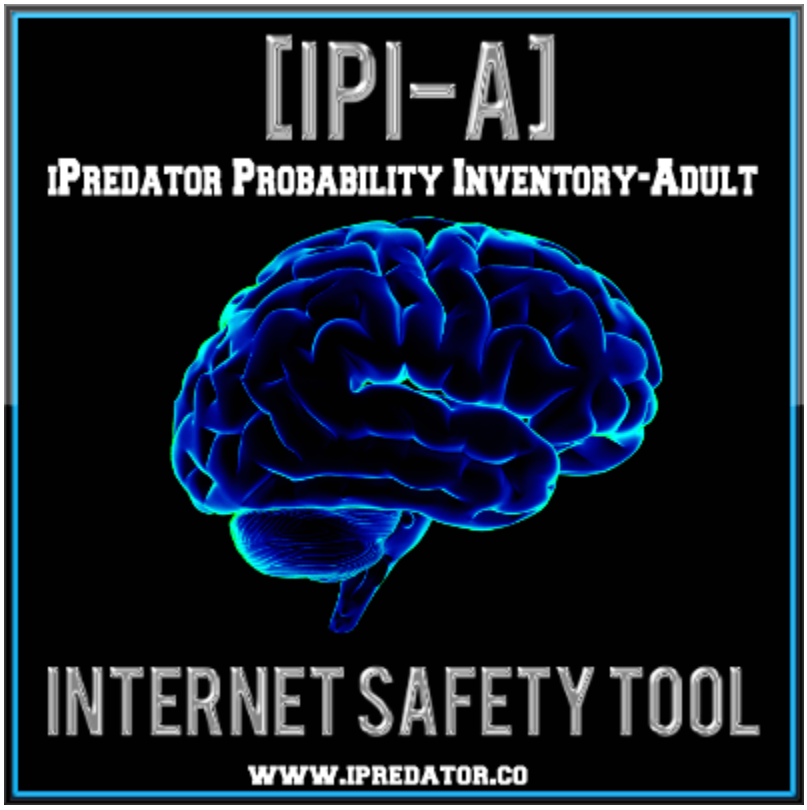
IPI-A

iPredator Probability Inventory - Adult

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



iPredator Probability Inventory - Adult (IPI-A)

The iPredator Probability Inventory-Adult is a 110-question diagnostic, education, assessment and data collection tool designed to investigate an adult's preparedness, vulnerability, risk potential and cyber-attack awareness. The IPI-A is also designed to assess an adult's preparedness of being assaulted, taunted, criminalized and/or victimized by iPredators based on their online activities and level of cautious approach.

Just as all the IPI Assessment Collection inventories, the IPI-A focuses on the adult's relationship to ICT, their knowledge base of malevolent and nefarious users, environmental aspects influencing their online activities. The IPI-A is completed by an adult age 18+.

Once completed, the IPI score, ranging from 0-110, represents an adult's vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyberstalking, cyber harassment or trolling for targets to sexually victimize. The IPI-A is also helpful to adults who are trying to learn and institute effective internet safety practices. For adults looking to evaluate their preparedness and vulnerability of an iPredator attack, the IPI-A was constructed to address these areas.

IPI-A DIRECTIONS

1. The time needed to complete the IPI-A inventory averages 60-90 minutes.

2. To complete the checklist, you must 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 ability 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 need 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.

IPI-A

Subject's Gender: Male__ Female__
Age: (18-32) __ (33-45) __ (46-54) __ (55-70) __ (71+) __
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. Has a peer or associate teased or harassed you online about personal information you have shared with others? NO
2. Have you been harassed or teased online based on you race, religion, socioeconomic status or sexual orientation? NO
3. Have you been "flamed" (mean, provocative or angry messages) and retaliated with equally angry responses? NO
4. Have you sent, posted or received disparaging messages about others and did not tell peers or associates? NO
5. Have you had an online relationship turn negative and they began harassing you? NO
6. Have you had secrets spread about you online? NO
7. Do you know how to help a peer, associate or loved one who is being cyber harassed by others? YES
8. Are you cautious about what you share online? YES
9. Do you protect your images and videos from online strangers viewing them? YES
10. Has an online user persistently harass or tease you and you retaliated by doing the same type of harassment or teasing? NO
11. Have you been or know someone who has been threatened, embarrassed, or teased online and you did not seek advice or professional help? NO
12. Within the last year, have you retaliated against someone online despite knowing it was not the correct approach? NO
13. Are you cautious disclosing personal information about yourself, your loved ones or co-workers? YES
14. Do you know what "*Digital Footprint*" means and how disclosing personal information can damage your credibility? YES
15. Have you shared confidential information to an ex-friend or associate and concerned about what they will do for revenge or control? NO
16. Do you have a positive "*Digital Reputation*" and know how to assess and maintain a positive one?" YES
17. Did you know that images and video you post online can remain in cyberspace for years? YES
18. Did you know sexual information you share online may be impossible to delete? YES
19. Did you know "*Sexting*" involving you or loved ones can be shared with without your consent? YES

20. Have you had sexual conversations with someone you met online and never met in person? NO
21. Do you tell your friends, coworkers and loved ones your passwords? NO
22. Have you called or taken phone calls from online strangers? NO
23. Have you ever been contacted by an online stranger and kept it a secret from loved ones? NO
24, Have you ever met an online stranger or associate in private offline for the first meeting? NO

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)

25. Do you respond to online strangers who initiate sexually themed contact? NO
26. Do you communicate with online strangers and keep it a secret? NO
27. Do you have a mobile device with information that is embarrassing or sexual? NO
28. Do you have a social profile set to "*public*" privacy settings that is not a fan, community or public figure page? NO
29. Do you visit high-risk websites (i.e. pornographic, racist, violent) and post your contact information? NO
30. Have you ever quickly shut off, logged out or closed your device because you did not want someone to know what you were doing online? NO
31. Are you educated on internet predators and cybercrime? YES
32. Are you aware iPredators target online users using kindness and understanding? YES
33. Do you know how cybercriminals engage in identity theft? YES
34. Do you know iPredators will encourage you to add them to your "*buddy*" and "*friend*" lists? YES
35. Do you give your passwords to loved ones you think you trust? NO
36. Do you know how to prevent unwanted access to your mobile devices? YES
37. Are you educated on the dangers of GPS location services? YES
38. Did you know GPS location services allow anyone to isolate your exact location at any given time? YES
39. Do you know how iPredators use attention and gifts to seduce online users? YES
40. Do you know iPredators may create profiles pretending to be someone you consider attractive? YES
41. Do you know what peer-to-peer networks are and how they can expose you to iPredators? YES
42. Has a loved one or professional expressed concern that you are online gaming addicted? NO
43. Did you know most online users are targeted by family members, family friends and trusted peers? YES
44. Are you suspicious of online users that encourage you to be defiant or deceptive to loved ones or coworkers? YES
45. Do you know iPredators look for targets who will access the internet during late night hours? YES

46. Do you spend time learning about "*Mobile Device Safety*"? YES
47. Do you know how to install & update security software on your mobile devices? YES
48. Do you follow school or work policies about mobile device usage? YES
49. Have you installed and updated antivirus software on your mobile devices? YES

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)

50. Do you share your passwords with loved ones who may not always be a loved one? NO
51. Do you post your home or cell phone numbers on sites available to the public? NO
52. Do you use multiple passwords and change them often? YES
53. Have you been confronted about the time you spend online gaming? NO
54. Do you visit "private" chatrooms or questionable websites and keep it a secret from loved ones? NO
55. Are you familiar with bot software, spyware, keystroke loggers and viruses? YES
56. Did you know that social media sites are frequented by iPredators with false identity profiles? YES
57. Have you contacted your phone carrier about security filters, controls and GPS services? YES
58. Are you prepared when associates or loved ones introduce you to questionable and high-risk websites? YES
59. Did you know that you can accidentally show your phone number by "*Caller ID*" to unknown entities? YES
60. Do you spend most of your waking like online? NO
61. Do you secretly search for sexual content involving minors? NO
62. Do you spend time surfing online when you are really upset? NO
63. Do you always log off and sign out when not using your email accounts? YES
64. Can you name three dangers of sharing your personal and/or contact information online? YES
65. Do any of your user accounts include your full or partial real name? NO
66. Do you know what *"Sextortion"* is and how to prevent online blackmail? YES
67. Does your best friend or lover know your passwords? NO
68. Do you click on links in emails from unknown senders? NO
69. Do you encourage your friends or loved ones to learn about internet safety? YES
70. Do you know what an *"Internet Troll"* is and how they target online users? YES
71. Do you have a plan of action in case you are habitually threatened online? YES
72. Do you check the sites you have joined to make sure personal information is not public? YES
73. Do you know why you never give your credit card information unless you are 100% sure the online payee is trustworthy? YES
74. Do you know how to recognize identity thieves pretending to be a reputable organization? YES

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)

75. Do you log directly into your institution's website when conducting academic, business or financial functions? YES
76. Do you send sensitive personal and/or financial information by email? NO
77. Do you ensure a site is secure and reputable before giving your credit/debit card number? YES
78. Do you only download legal files, music and videos & aware of online piracy? YES
79. Do you spend less time with friends, family, and more time online? NO
80. Do you have an online cut-off time if it will interfere with school or work? YES
81. Would you talk to a loved one or professional if you felt distressed or angry due to your online activities? YES
82. Do you feel angry, anxious or sad due to not having enough online time? NO
83. Do you feel more comfortable online rather than spending time with family? NO
84. Have you become less interested in your favorite offline activities due to increased interest in your online activities? NO
85. Has loved ones or coworkers said you have changed or isolating due to your online activities? NO
86. Are you angry or stressed due to being confronted about the amount of time you spend online? NO
87. Do you read and understand refund, return and guarantee policies when shopping online? YES
88. Do you check consumer reporting sites to decide the legitimacy of a company you are interested in doing business with? YES
89. Do you engage in online or offline risk-taking and have been confronted by loved ones? NO
90. Have you been less attentive, less productive or falling behind in school, work or major responsibilities due to your online activities? NO
91. Do you have a social media account that you access more than 20 times a day? NO
92. Do you regularly check your privacy and account settings? YES
93. Do you allow others you do not know join your "*friends*" list? NO
94. Do you limit who can view your images and videos at your social profile page? YES
95. Do you spend large periods of time involved with social sites that have no academic or career benefits? NO
96. Do you have a social media profile with contact information available to the public? NO
97. Have you shared personal details online that a loved one would feel is dangerous? NO
98. Do you share your email or home address with online strangers? NO
99. Do you review the number of social media "*friends*" you have and accept online strangers looking to increase the total number? NO
100. Do you restrict your images and videos for public consumption? YES
101. Do you have a genderless and asexual screen name to hide your gender or ease of identification? YES

102. Do you have a safe e-mail address that does not give away personal information about your identity or location? YES
103. Do you click on unknown links and attachments in unfamiliar emails? NO
104. Do you know your state cyberstalking and cyber harassment laws? YES
105. Do you refrain from showing your home address when visiting chatrooms, message boards and forums? YES
106. Do you protect all devices with secure passwords that are difficult to guess? YES
107. Do you continually change your passwords on all ICT accounts? YES
108. Are you always suspicious of incoming emails, telephone calls or text messages that ask for personal identifying information? YES
109. Do you give out your Social Security Number online? NO
110. Do you neglect your work, school or family responsibilities due to time spent online? NO

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)

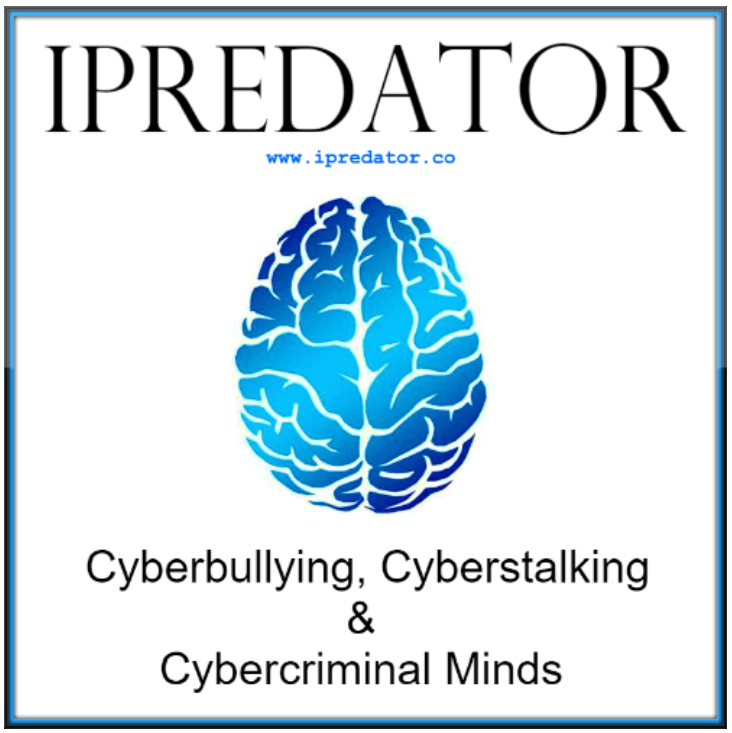
Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Correct Responses__+ Does Not Apply Responses__= IPI-A Score

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 at once with a plan of action. Although obtaining a score of 100 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. As information and communications technology expands, it will become increasingly important to manage and monitor cyber-attack prevention, digital citizenship and 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 this inventory on a quarterly basis and more often 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 online users are very real and can range from frustrating to deadly.



IISC SCORE DEFINITION

IISC Score: Upon completion of any of the IISC assessments, the respondent will have a final score ranging from 0-75, 0-110 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.

IPI SCORING KEY

IPI Score: (1-10)
Category: Guaranteed iPredator Target
Risk Potential: Alarmingly High
iPredator Involvement: Certain
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Urgent Attention Required

IPI Score: (11-29)
Category: Prime iPredator Target
Risk Potential: High
iPredator Involvement: Almost Certain
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Immediate Attention Required

IPI Score: (30-39)
Category: Probable iPredator Target
Risk Potential: Moderately High
iPredator Involvement: Involvement Likely
Intervention Plan: Professional Consultation Highly Advised
Level of Urgency: Immediate Attention Strongly Recommended

IPI Score: (40-55)
Category: Likely iPredator Target
Risk Potential: Moderate
iPredator Involvement: Involvement Suspected
Intervention Plan: Create and Implement an iPredator Prevention Plan
Level of Urgency: Immediate Attention Recommended

IPI Score: (56-69)
Category: Possible iPredator Target
Risk Potential: Moderate
iPredator Involvement: Involvement Possible
Intervention Plan: Increase iPredator Protection & Prevention Strategies
Level of Urgency: Immediate Attention Suggested

IPI Score: (70-84)
Category: Skilled iPredator Protection with 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 Below 80

IPI Score: (90-110)
Category: Advanced iPredator Protection with Minimal Vulnerability
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.