IPI-CS

iPredator Probability Inventory - Cyberstalking

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

iPredator Probability Inventory - Cyberstalking (IPI-CS)

The iPredator Probability Inventory - Cyberstalking is a 110-question diagnostic, education, assessment and data collection tool designed to assess the probability and preparedness of a young adult, adult or public figure of being cyberstalked. In addition to cyberstalking, the IPI-CS investigates the subject's potential of being cyber harassed by an ex-partner, ex-associate, fan, nefarious corporate entity or pathologically driven online user. Just as all the IPI Assessment Collection inventories, the IPI-CS focuses on the subject's relationship to ICT, their knowledge base of malevolent and nefarious users, environmental aspects influencing their online activities and their practice of the behavioral actions necessary for Internet safety and preparedness if cyber attacked.

An adult, public figure or associate of a public figure age 18+ completes the IPI-CS. Once completed, the IPI score, ranging from 0-110, represents the inventory respondent's or the subject being queried preparedness, vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyber stalking, cyber harassment or cyber bullying if the subject being queried is a minor. The IPI-CS can be used as both a cyberstalking prevention tool and data collection instrument if the online user or business is presently being cyberstalked. The IPI-CS also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-CS DIRECTIONS

1. The time required to complete the IPI-CS inventory 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.

IPI-CS

Subjects Gender: Male__ Female__ N/A__
Age: Teen (18-20) __Young Adult (21-25) __Adult (26+) __Business__
Average Daily Online Activity: 0-1 Hour__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. Do you consistently ignore "flaming" (provocative or angry online messages) from a suspected, confirmed or unidentified cyberstalker?

2. Can you, a loved one or responsible employee confirm you have genderless and nameless screen names, email account addresses, website/blog domain names and social site usernames when given the option?

3. Do you consistently disseminate minimal identifiable information online when given the option?

4. Do you review your home state and frequently visited area cyberstalking, cyberbullying and cyber harassment laws?

5. Do you not disclose permanent and temporary housing locations and event appearances when allowable?

6. Do you password protect your ICT using secure passwords that are difficult to decrypt, even for the most tenacious cyberstalkers?

7. Do you change your passwords regularly and make password "hints" difficult to decipher on all ICT accounts and devices?

8. Do you consistently delete or erase incoming emails, phone calls, tweets and text messages that inquire about your present and future geographic locations without a logical reason?

9. Do you refrain from disclosing your social security # and street address # unless required by a verified online source?

10. Do you actively monitor website stat counters that will record all incoming traffic to your blogs, websites and online content?

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)

11. Do you regularly check your credit reports and account balances for identity theft and/or suspicious activities?

12. Do you actively monitor cyberstalker surveillance tactics, devices and software installed on your ICT or checked by surveillance and tracking technology professionals?

13. Do you refrain from sharing contacts and financial information in all online messages and transmissions and chatroom correspondences?

14. Do you decline meeting online acquaintances in person without first having their identity fully verified first?

15. Do you verify that ISP and Internet Relay Chat (IRC) networks have acceptable use policies prohibiting cyberstalking?

16. Do you contact law enforcement then exit from online situations, which become hostile, bizarre or sexually inappropriate?

17. Do you document all ICT communications initiated by a cyberstalker, internet troll or hostile ex-partner?

18. Do you keep records of contacts with internet system administrators and law enforcement if cyberstalked, harassed or taunted by an ex-partner?

19. Do you know how to block or filter all ICT device messages from a cyberstalker or non-contact ordered ex-partner?

20. Do you know how to report a cyberstalker, internet troll or ex-partner to an Internet Service Provider (ISP)?

21. Do you know how to compile evidence of cyberstalkers, ex-partners and internet trolls who post felonious sexual images of you and your loved ones online?

22. Do you know when to contact authorities and inform them in detail if cyberstalked, harassed or taunted by an ex-partner?

23. Do you know how to distinguish the differences between the tactics of cyberstalking and the pathology of an obsessed stalker?

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. Do you regularly review "friend" or "buddy" lists and remove contacts that are not actual friends, trusted associates or public figure followers?

25. Do you delete applications no longer or rarely used, given they have access to your personal information?

26. Do you know what to do if harassing or unwanted communications via ICT from an ex-partner, ex-associate, fan or competitor becomes distressing?

27. Do you know cyberstalkers impersonate their victims and attack others online the victim knows?

28. Do you know to inform a cyberstalker that you would like him or her refrain from contacting you and documenting the dates, times and details of the requests?

29. Do you know not to respond to emails or text messages from an ex-partner, acquaintance or stranger engaging in hostile or bizarre behaviors?

30. Do you know that receiving unsolicited threatening emails and/or death threats in most states is defined as criminal aggravated harassment?

31. Do you know what to do if infected by electronic viruses sent from an ex-partner, acquaintance, stranger or fan?

32. Do you know how to intervene if spam has been sent from a disgruntled ex-partner, acquaintance, stranger or fan?

33. Do you know how to intervene if sexually harassed in online posts, email messages, voicemails or text messages?

34. Do you know how to intervene if cyber harassed or threatened in chatrooms, forum posts and message boards?

35. Do you know what to do if your personal information is posted by a disgruntled ex-partner, acquaintance or stranger without your consent?

36. Do you know what to do if your email account has been hacked by a disgruntled ex-partner, acquaintance or stranger?

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)

37. Do you know what to do if you are subscribed to pornography websites or distasteful advertising without your consent by a disgruntled ex-partner, acquaintance or stranger?

38. Do you regularly check if spyware on your ICT devices have been installed by an ex-partner, ex-associate, fan or competitor?

39. Do you check if being tracked by GPS technology?

40. Do you know how to check if your phone calls or messages are being intercepted?

41. Do you know what to do if being impersonated online by an ex-partner, ex-associate, fan or competitor?

42. Do you know how to recognize and what to do if being watched by hidden cameras or covert video equipment?

43. Do you know if being stalked or harassed by a stranger, there is a good chance it is an ex-partner, acquaintance or fan?

44. Do you know what to do if a cyberstalker contacts your family, employer or associates without your consent or knowledge?

45. Do you know that online users who post personal information when blogging have higher rates of being cyberstalked and harassed?

46. Do you know cyberstalkers, obsessed fans and ex-partners follow their targets from site to site?

47. Do you make sure email addresses, instant messaging usernames and links to personal homepages cannot be directly connected to you, a loved one or associate?

48. Do you know online users are particularly susceptible to cyberstalking and harassment if actively video blogging (vlogging?)

49. Do you know a cyberstalker can be an ex-partner, obsessed lover, fan, ex-employee or someone with a grudge due to a minor or imagined reason?

50. Do you know cyberstalkers inconspicuously pose as friends, associates or fans online asking innocuous questions they will use to attempt recovering your passwords?

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. Do you know that most cyberstalking and harassment involves someone you know or have interacted with your immediate past?

52. Do you know that cyberstalking can occur whether the offender and target reside, socialize or work in the same geographic location?

53. Do you know a cyberstalker can be an egotistic aggressor who wants to show-off to their peers by habitually causing you distress?

54. Do you avoid announcing the physical location by your GPS-enabled applications via status updates?

55. Do you know changing internet service providers and reporting the distressing events to authorities is recommended to stop cyberstalking and harassment?

56. Do you know it is recommended to contact your local FBI Computer Crimes Unit if cyberstalked, threatened or harassed?

57. Do you make sure to log out of your computer if you will be unavailable for extended periods?

58. Do you know what to do if someone sends threatening, lewd or harassing emails from an assortment of email accounts?

59. Do you know what to do if your settings and passwords have been changed in your online accounts?

60. Do you know what to do if someone posts messages to online bulletin boards and discussion groups with your banking information embedded in the messages?

61. Do you know cyberstalkers impersonate their victim and post lewd or controversial information?

62. Do you know what to do if signed up to online mailing lists and services without your consent?

63. Do you know your state cyberstalking and cyber harassment laws?

64. Do you refrain from using gender specific or provocative screen names?

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)

65. Do you refrain from flirting or arguing online?

66. Do you know how a cyberstalker can find their victim by gaining access to their accounts of already-established connections (i.e. Facebook friends or Twitter followers?)

67. Do you know to warn friends and acquaintances not to post yours or their contact information and location online?

68. Do you know not to post images of your home that might indicate its location by showing a house number or an identifying landmark in the background?

69. Do you know to use caution when joining online organizations, groups or "fan pages" and never publicly RSVP to events shown online?

70. Do you know to use caution when connecting a mobile phone to a social networking account?

71. Do you know to avoid posting information about your current or future locations, such as a review of a restaurant you have posted near your house?

72. Do you know to only post information that would not expose you to harm if a cyberstalker or harasser should read it?

73. Do you know that both cyberstalking and physical stalking can lead to a physical attack and you should always get help quickly?

74. Do you know whether you live in a state that requires that the perpetrator, to qualify as a stalker, make a credible threat of violence or only that their conduct constitutes an implied threat?

75. Do you have an emergency cash fund to take time from work to change a phone number, move, replace damaged property, obtain a restraining order or testify in court?

76. Do you know cyberstalkers may commit identity theft by opening or closing accounts, taking funds or charging purchases to your credit card?

77. Have you, a loved one or responsible employee researched to see if your state has an address confidentiality program for those who are being targeted by cyberstalkers?

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)

78. Have you, a loved one or responsible employee made sure you have an unlisted phone number that is still unlisted and not returned to public status, which inadvertently happens on occasion?

79. Have you, a loved one or responsible employee signed up for "Caller ID Complete Blocking" also called "Per Line" blocking?

80. Have you, a loved one or responsible employee purchased a pre-paid cellular phone with cash if required to protect yourself from a cyberstalker or disgruntled ex-partner required to leave the area in an emergency?

81. Do you actively conduct internet searches using your name and phone number to see if the cyberstalker or your ex-partner is engaging in nefarious online activities using your identity?

82. Do you avoid calling toll-free number services because your phone number can be "captured" by a service called Automatic Number Identification?

83. Do you know how to have your name removed from "reverse directories"?

84. Do you know to never use your residential address for anything that is mailed or shipped to you if concerned about a cyberstalker hostile ex-partner?

85. Do you refrain from using the middle initial of your middle name since middle initials are often used to differentiate people with common names?

86. Do you only fill in pieces of information that are required when completing online forms?

87. Do you know you can use a post office box on your driver's license as opposed to using your actual home address?

88. Do you know not to put your name on the list of tenants on the front of your apartment building and use a variation of your name that only your friends and family will recognize?

89. Do you know the Social Security Administration may be willing to change your Social Security #?

90. Do you know how to alert the three credit bureaus (Experian, Equifax and Trans Union) to put a fraud alert on your credit reports to avoid fraudulent access and freezing?

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)

91. Do you keep a log of every cyberstalking, hostile and harassing incident for presentation to authorities if required as evidence?

92. Do you know to be cautious about applying for a domain name using your name as the site domain name?

93. Do you know, if you have a domain name, to register it as private so your personal information is not available to the public?

94. Do you know how to contact your state victim's advocacy office for help filing a court-issued restraining order against a cyberstalker or disgruntled ex-partner?

95. Do you know how to set up email alerts with search engines that alerts you if your identity is actively being disseminated by a cyberstalker or ex-partner without your consent?

96. Do you know how to deactivate your Twitter account if concerned about being cyberstalked or harassed?

97. Do you know how to access the privacy settings in your Twitter account to maximum privacy?

98. Do you know how to block a cyberstalker or harasser and report them to Twitter?

99. Do you know to avoid clicking on redirect links from Twitter followers you do not trust or cannot verify their identity?

100. Do you know to always make sure you are visiting the real Twitter by checking the URL?

101. Do you refrain from posting or sharing personal information online that is provocative, violent, sexually suggestive or age inappropriate?

102. Do you refrain from interacting with online strangers in chatrooms that are not moderated?

103. Do you regularly scan your ICT using anti-virus software for viruses that a cyberstalker may have sent you without your knowledge.

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)

104. Do you know to practice extreme cautious about meeting online acquaintances in person?

105. Do you remind you to refrain from engaging in flirting or sexually suggestive discussions online?

106. Do you regularly Google your name or brand to make sure no personal information is posted by others about you that is felonious or disparaging?

107. Do you know to refrain from confronting a cyberstalker in a hostile manner as it only arouses them for more angry or emotional attacks?

108. Are you, a loved one or responsible employee selective with whom you accept onto your social media pages and profiles?

109. Do you know how to disable location devices or GPS that tags your photos with a location?

110. Do you consistently refrain from posting your daily activities and upcoming events that you will be attending at social networking sites?

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

Yes Answers __ No Answers __ I Do Not Know__ Does Not Apply__

Correct Responses__+ Does Not Apply Responses__= IPI 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 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. 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 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 online users are very real and can range from frustrating to deadly".
Michael Nuccitelli Psy.D.

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.