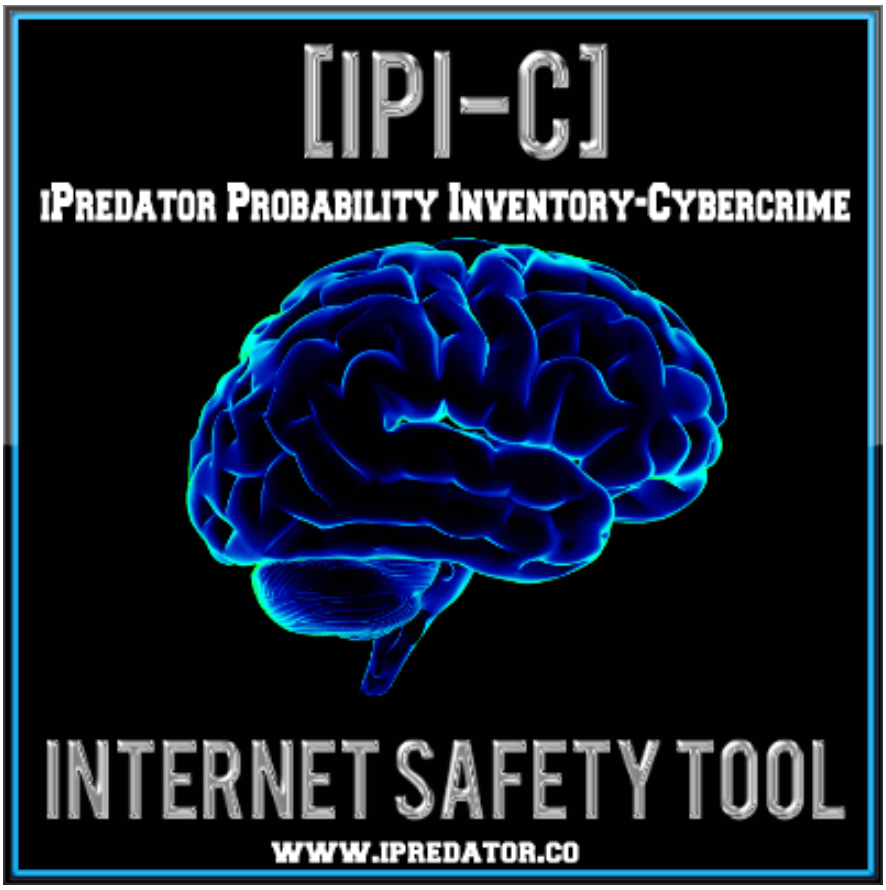
IPI-C

iPredator Probability Inventory - Cybercrime

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



iPredator Probability Inventory - Cybercrime (IPI-C)

The iPredator Probability Inventory - Cybercrime is a 110-question diagnostic, education, assessment and data collection tool designed to assess and investigate an adult or business's probability of being targeted, disparaged, stolen from or infiltrated by iPredators or nefarious corporate competitors engaged in cybercriminal activities. An adult age 18+, business owner or corporate associate familiar with the business's health and safety completes the IPI-C.

Once completed, the IPI score, ranging from 0-110, represents the vulnerability, preparedness and risk potential of the adult or business being targeted by an iPredator engaged in cybercrime. Areas focused on in the IPI-C include identity theft, personal and financial information protection, ICT safety and cyber security. In addition to a diagnostic and data collection tool, the IPI-C can also be used to assist an online user or a business to investigate their security breach weaknesses if they have been victimized by cybercrime. The IPI-C also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-C DIRECTIONS

1. The time required to complete the IPI-C 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-C

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__

Information and Communications Technology = ICT

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. Is your ICT safe from hackers and checked regularly for updates that are current with the latest patches and updates?
YES

2. Is your ICT safe from viruses and checked regularly to ensure that you or your business have configured your web browsers and email software set to the strongest security settings?
YES

3. Is your ICT safe by confirming that you do not have software flaws (vulnerabilities) that may open your ICT to cyber-attacks?
YES

4. Is your ICT safe from a mobile device cyber-security breach and checked regularly for updates, patches and software flaws?
YES

5. Do you or your business have a formal or informal written internet security plan and regularly evaluate your ICT security needs?
YES

6. Do you or your business participate in internet safety training or online self-education to ensure you are aware of new cyber-attacks threats?
YES

7. Does your ICT get automatic software and security updates, and do you confirm your firewalls are properly activated and ant-spyware software is functioning properly?
YES

8. Do you or your business regularly inspect the information you have stored on all ICT devices and what is required to protect that information or wiped if unnecessary?
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)

9. Do you or your business regularly inspect how you store and protect data on mobile devices and pay close attention to wiping all unnecessary data not relevant as well as sensitive information?
YES

10. Do you or your business regularly inspect how you, loved ones or employees access and share personal information at social networking sites?
YES

11. Do you or your business regularly assess what new privacy settings you may need at social networking sites?
YES

12. Do you or your business make sure your operating systems have the latest system updates or confirm operating systems are set to automatic updates?
YES

13. Do you or your business know how to safely and securely use the internet and how it can lead to cybercrime if not used in a cautious manner?
YES

14. Are you or your business aware of what websites and social networking sites are being visited during downtime at the workplace or at your home connected to work or school?
YES

15. Are you or your business educated on safe online practices and know who to contact immediately if hacked or cyber attacked?
YES

16. Do you or your business diversify your passwords on all ICT devices and ensure they cannot be easily decrypted?
YES

17. Are you or your business aware of the latest security threats, how to combat them and have available a certified internet security professional for prompt access if needed?
YES

18. Are you or your business safe from a loss of data and identity theft, checked regularly and only use websites that are secure prior to submitting your credit card number or financials?
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)

19. Are you or your business safe from loss of customer or personal information that is confirmed by regularly inspecting all ICT devices for cyber-attack vulnerabilities?
YES

20. Do you, your loved ones or business have guidelines or rules on how long to keep documents with financial information before backing up, wiping or deletion?
YES

21. Do you, your loved ones or business have social networking site guidelines on what information and content is permissible to share online and using mobile devices?
YES

22. Do you, your loved ones or business have social networking site guidelines on how to safeguard private, personal and/or financial information?
YES

23. Do you or your business review your credit reports quarterly or at least once per annum to verify no fraudulent activities have occurred?
YES

24. Do you or your business have a customized cyber security plan or at least researched what a customized cyber security plan entails?
YES

25. Do you or your business have passwords that are complex, not easily decrypted, intermittently changed and both themed genderless and nameless?
YES

26. Do you disclose online or when using mobile devices, financial information about your business, employer or family?
NO

27. Do you or the business have a security strategy that is multi-layered with numerous obstacles discouraging cyber criminals and intruders for infiltrating your ICT?
YES

28. Have you or the business neglected to plan or not initiated a cyber security plan in preparation of a cyber-attack?
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)

29. Do you know how to report and reduce damages from hacking, stolen finances or identity theft that is both effective and up to date taking into consideration new cybercrime tactics?
YES

30. Do you, your loved ones or business have an internet usage policy, formal or informal, that explains the websites and web services you, employees and loved ones can use for all ICT devices.
YES

31. Do you, your loved ones or business have a plan in place if you suffer a data breach or loss of personal, family, customer or employee information that includes mobile device safety?
YES

32. Do you or your business inform loved ones, customers or partners/suppliers how you protect their personal and financial information if consumer satisfaction is a business objective?
YES

33. Do you, your loved ones or business keep up with the increasing adoption of mobile and social media platforms placing a priority on safety and security measures?
YES

34. Do you have guidelines for yourself, employees and/or family member's use of social media and social networking sites regarding privacy settings?
YES

35. Are you or your businesses prepared for and safe from the cyber-attack called social engineering?
YES

36. Do you, your loved ones or business keep up with news on increasing smartphone and mobile device security vulnerabilities that are specific to the mobile device brands you are using?
YES

37. Do you, your loved ones or business use multifactor authentication to access your networks?
YES

38. Do you, your loved ones or business completely wipe data off your ICT devices before disposing them?
YES

39. Do you or your business regularly confirm security measures are installed, updated and functional at all entry points?
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)

40. Do you have or create user screen names that are suggestive and/or refer to your age, sex, gender or location?
NO

41. Do you monitor your credit statements monthly for any fraudulent activity and always obtain a physical address of the seller when making an online purchase?
YES

42. Do you, your loved ones or employees communicate with online strangers or businesses that have not verified as credible and reliable?
NO

43. Do you or your business have passwords with less than five characters for convenience?
NO

44. Do you or your business use the same password at websites, social sites, service providers and email account?
NO

45. Do you, your loved ones or business consistently type in the website address rather than clicking on a link provided?
YES

46. Do you, your loved ones or employees neglect to always look for the "locked" icon at e-commerce & m-commerce sites?
NO

47. Do you, your loved ones or employees regularly make sure computers are configured securely and the correctness of the claimed identity you are interacting with has been confirmed?
YES

48. Do you, your loved ones or employees respond to unknown email messages asking for personal information or containing unknown attachments?
NO

49. Are you, your loved ones or employees educated on preventing Internet and Escrow Services Fraud?
YES

50. Are you, your loved ones or business aware that prompt and effective action is critical to protecting online personal and corporate reputation?
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)

51. Do you or your business encrypt all hard drives and IVT devices to help protect vital data in case of theft or loss?
YES

52. Do you, your loved ones or business use a pass code on mobile devices and subscribe to a remote wipe service for protecting data if loss or stolen?
YES

53. Do you, your loved ones or business know what personal and financial information are stored in files, computers and mobile devices that are safely backed up to a secure central database?
YES

54. Do you, your loved ones or business consistently monitor whom, and in what capacity, send sensitive personal information from your home, business and social media sites?
YES

55. Do you, your loved ones or business identify whether your servers are utilizing ports that have been previously known to represent insecurities?
YES

56. Do you, your loved ones or business know where you keep information collected at each entry point (i.e. central computer database, individual laptops, disks, tapes, cloud etc.)?
YES

57. Do you, your loved ones or business always avoid filling out forms in email messages asking for personal information?
YES

58. Do you, your loved ones or business delete, shred and destroy personal or customer credit card information unless it has a relevant or business need?
YES

59. Do you, your loved ones or business have a data security plan that includes physical security, electronic security, employee training and the security practices of contractors and service providers?
YES

60. Can you, your loved ones or business identify the computers or servers where sensitive personal information is stored quickly if cyber attacked?
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)

61. Can you, your loved ones or business identify all connections to the ICT devices where you store sensitive information?
YES

62. Do you, your loved ones or business regularly assess the vulnerability of social media profiles that are known to experience cyber-attacks?
YES

63. Do you, your loved ones or business minimize as best the storage of sensitive financial or consumer data on ICT devices unless it is essential?
YES

64. Do you, your loved ones or business regularly check information security websites and software vendor websites for alerts about new vulnerabilities specific to your ICT devices
YES

65. Do you, your loved ones or business scan the computers on your network to identify and profile the operating system and open network services?
YES

66. Do you, your loved ones or business receive and transmit credit card information or other sensitive financial data using Secure Sockets Layer (SSL) protecting the information in transit?
YES

67. Do you, your loved ones or business use "password activated" screensavers to lock ICT devices after a period of inactivity?
YES

68. Do you, your loved ones or business lock out guest users who do not enter their correct password within a designated number of log-on attempts?
YES

69. Do you, your loved ones or employees immediately change vendor-supplied default passwords when installing new software?
YES

70. Do you, your loved ones or employees restrict the use of laptops to those who need them to perform their jobs or academics?
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)

71. Do you, your loved ones or employees store all ICT devices in a secure place?
YES

72. Do you require family members or employees to immediately notify you if there is a potential security breach, such as a lost or stolen laptop?
YES

73. Do you or your employees investigate security incidents at a leisure pace and not take steps to close off existing ICT vulnerabilities?
NO

74. Do you, your loved ones or employees' password protect all ICT devices that hold sensitive data and properly encrypt them?
YES

75. Do you, your loved ones or employees often forget to securely back up stored data from mobile devices and do not subscribe to remote wipe services?
NO

76. Do you, your loved ones or employees often misplace portable electronic devices and do not subscribe to remote wipe services?
NO

77. Do you, your loved ones or employees forget to turn off wireless services when they are not being used for extended periods?
NO

78. Do you; your loved ones or employees keep your mobile device security plan current by having the latest software updates, anti-spyware, operating systems and remote wipe services?
YES

79. Do you, your loved ones or employees review the privacy policy on mobile devices an application can access before it is downloaded?
YES

80. Do you, your loved ones or employees know how to disable the geotagging feature on 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)

81. Do you, your loved ones or employees know about Wi-Fi hotspots and types of financial & business functions to limit?
YES

82. Do you, your loved ones or employees know when banking or shopping, using mobile devices, to look for web addresses with "https://" or "shttp://"?
YES

83. Are you, your loved ones or business familiar and protected from credit card fraud?
YES

84. Are you, your loved ones or business familiar and protected from identity theft?
YES

85. Are you, your loved ones or business able to recognize and are familiar with DHL/UPS scams?
YES

86. Are you, your loved ones or business able to recognize and are familiar with Escrow Services Fraud?
YES

87. Are you, your loved ones or business able to recognize and are familiar with Internet Extortion?
YES

88. Do you, your loved ones or business attempt to calculate the minimal amount of information you must provide online to successfully complete a transaction?
YES

89. Do you, your loved ones or business contact the seller with questions before you bidding on auction sites or when purchasing merchandise online?
YES

90. Are you, your loved ones or business cautious and request verification when dealing with individuals or companies outside of your own country?
YES

91. Do you, your loved ones or business sporadically forget to ensure a website is secure and reputable before providing your financial information 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)

92. Do you, your loved ones or business feel comfortable providing your credit card information when requested through unsolicited emails?
NO

93. Do you, your loved ones or business contact the Better Business Bureau or other consumer protection organizations to determine the legitimacy of a company?
YES

94. Are you, your loved ones or business wary of businesses that operate from P.O. boxes or mail drops?
YES

95. Do you, your loved ones or business always type in the website address of unknown origin or identity rather than clicking on a link provided for opening?
YES

96. Are you, your loved ones or business cautious when a site requests payment to an "agent", instead of a corporate entity?
YES

97. Do you, your loved ones or business ensure websites are secure prior to submitting a credit card number?
YES

98. Do you, your loved ones or business report unauthorized financial transactions to your bank or credit card company, once found, and as soon as possible?
YES

99. Do you, your loved ones or business first make sure nobody is watching when using public kiosks to check email and entering login information.

100. Do you, your loved ones or business assume a company is legitimate based solely on the "appearance" of their website?
NO

101. Do you, your loved ones or business fill out forms in email messages that ask for personal information?
NO

102. Do you, your loved ones or business personally log on to an official website you are interested in, instead of "linking" to it from an unsolicited email?
YES

103. Do you, your loved ones or business respond to spam, confirming to the sender, that it is a "live" email address?
NO

104. Do you, your loved ones or business regularly review bank and credit card statements for fraudulent activities and know what steps to take if identify theft has occurred?
YES

105. Do you, your loved ones or business know to never conduct any financial transactions, including online banking or purchases, over an unsecured wireless network?
YES

106. Do you, your loved ones or business pay close attention to privacy policies on websites and before installing new software for your ICT?
YES

107. Do you, your loved ones or business confirm that your bank uses fraud prevention systems that call out unusual purchasing behavior?
YES

108. Do you, your loved ones or business turn off ICT devices if they are not being used for extended periods?
YES

109. Do you, your loved ones or business check new cybercrime protection product availability that is specific to the ICT you are using?
YES

110. Do you, your loved ones or business diversify your passwords?
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)

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

Correct Responses__+ Does Not Apply Responses__= IPI-C 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.

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.