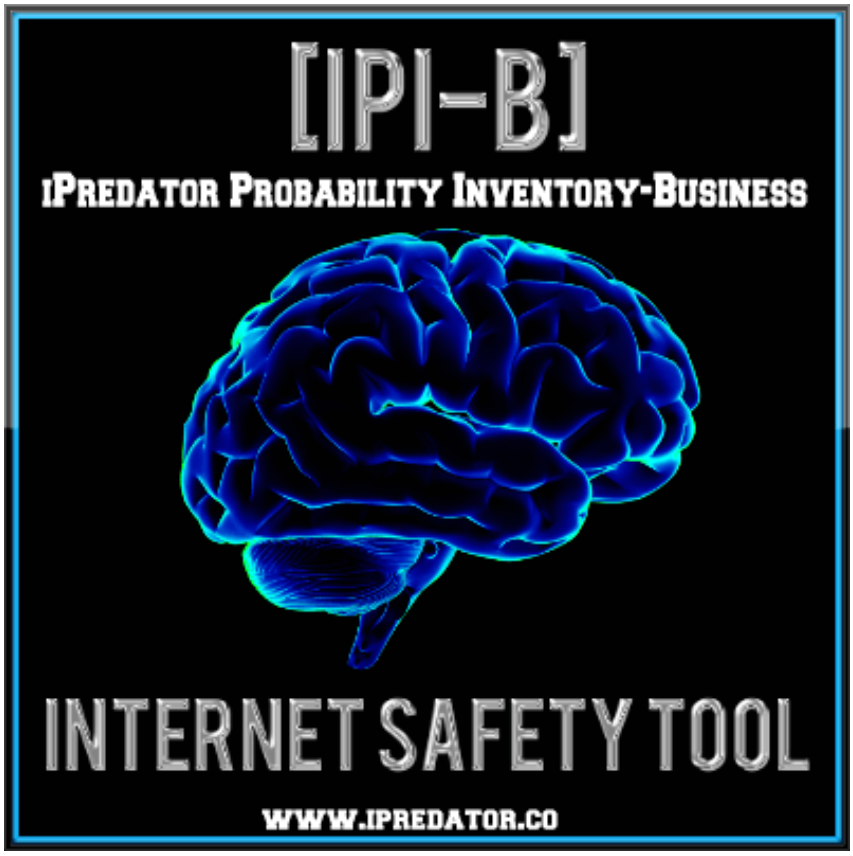
IPI-B

iPredator Probability Inventory - Business

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



iPredator Probability Inventory - Business (IPI-B)

The iPredator Probability Inventory-Business is a 110-question diagnostic, education, assessment and data collection tool designed to assess a business's vulnerability of being targeted, disparaged, slandered, stolen from or infiltrated by iPredators or nefarious corporate competitors. Related to cybercrime specific areas, the IPI-B also assesses a business's cyber-security breach potential, digital reputation acumen and capacity to institute Internet safety and cyber security strategies. A business owner, employee or consultant familiar with the business's information and communications technology (ICT) health and safety completes the IPI-B.

Relevant to businesses, the IPI-B addresses and investigates the businesses understanding of digital reputation and digital reputation management. Upon completion of the IPI-B, the IPI score ranges from 0-110 and represent the vulnerability and risk potential if targeted by an iPredator or nefarious corporate competitor engaged in cybercriminal activity and/or corporate disparagement. The IPI-B is a helpful diagnostic and educational tool for employees and consultants related to the business. The IPI-B also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

IPI-B DIRECTIONS

1. The time needed to complete the IPI-B 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-B

Note: The term "business" in the IPI-B represents any of the following: owner(s), employees, business consultants or the business itself as an entity.

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 the business ICT cyber security protected with regular cyber security monitoring to prevent damaging cyber-attacks by hackers, nefarious corporate competitors, ex-employees, disgruntled customers and checked regularly for updates?

2. Is the business ICT cyber security protected from business/consumer database financial information infiltration, identity theft and actively checked by the business?

3. Is the business ICT cyber security protected from malware infections and checked regularly for security updates and newly attacking viruses?

4. Is the business ICT safe from a mobile device security breach and checked regularly for updates?

5. Does the business have a formal written internet security policy available and given to all employees along with regularly scheduled employee trainings on cyber-attack prevention?

6. Does the business engage in Internet safety training for employees that includes both on-site and off-site internet safety measures to protect the business?

7. Does the business's ICT have automatic software and security updates that is monitored by an employee to ensure optimal cyber security functioning?

8. Does the business actively inspect sensitive online information and mandatory requirements for protecting the business and the customer databases?

9. Does the business actively protect sensitive data on mobile devices and conduct trainings for employees on mobile device safety?

10. Does the business monitor how employees interact with social media including both the business's social media interactions and the employee's personal social media interactions in respect to discussing company operations?

11. Does the business regularly check new cybercrime tactics that target corporate environments and how to prevent cybercriminal attacks and protection products?

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)

12. Does the business actively monitor sensitive customer information and recognize the value to cyber criminals who succeed in customer database infiltration?

13. Do the business partners and employees know the damaging consequences of using the Internet & mobile devices in an unsafe and haphazard manner?

14. Does the business track social networking sites employees visit during downtime at the job site coupled with clearly documented policies for employees on social media usage?

15. Is the business educated on safe online practices and customer relations techniques to reduce cyber-attacks by disgruntled consumers?

16. Does the business diversify the company ICT passwords and mandate employees to not disclose company passwords to non-employees of the business?

17. Does the business stay abreast of the latest cyber security threats along with digital reputation monitoring?

18. Is the business confidently safe from loss of financial data due to technology disruption, employee error and cyber-attacks?

19. Is the business safe from customer and financial information theft and the necessary steps needed if targeted by cyber criminals?

20. Is the business safe from all technological and human error events leading to loss of sensitive employee and financial data with the most recent successful confirmation being within the last quarter?

21. Does the business have formal written and reviewed guidelines on how long to keep online documents paying close attention to financial data documents?

22. Does the business have social media guidelines on what is permissible to share online by employees, consultants and business affiliated agencies?

23. Does the business know how to safeguard private, personal and financial information by monitoring employee surfing habits using software-based solutions?

24. Does the business inform consultants and employees about cyber security strategies and cyber-attack tactics if corporate competitors are suspected of being assailants?

25. Does the business have a customized cyber security plan that is issued to all employees and consultants as well as intermittently reviewed and updated?

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. Does the business have complex passwords that are not easily decrypted and monitored by trusted employees?

27. Does the business understand the importance of not disclosing financial information online unless necessary and maintain regular contact with the business's financial institutions regarding cyber security policies and procedures?

28. Does the business limit and tailor access to ICT of employees and consultants to reduce the risk of an internal breach?

29. Does the business have a formal emergency plan for possible cyber-attacks that can be immediately implemented reducing corporate and customer damages?

30. Does the business have structured steps for employees on how to report hacking, stolen finances or identity theft if cyber attacked?

31. Does the business have a formal Internet security policy for employees that are intermittently reviewed by all employees and those adept at cyber security strategies?

32. Does the business have an Internet usage policy clarifying what websites and web services employees can use during working hours?

33. Does the business check social media comments about the business disseminated by employees, past and present customers and competitors?

34. Does the business have a formal prevention and intervention plan if there is a data breach or loss of customer and employee information to insulate the business from possible civil litigation?

35. Does the business inform customers and partners/suppliers how it works to protect their information from cyber criminals and nefarious online users?

36. Does the business know cyber criminals are increasingly targeting businesses with minimal internet safety protection using a variety of methods to probe a business's weaknesses?

37. Does the business stay abreast of new mobile and social media platforms that can boost lead generation and monitor digital reputation?

38. Does the business have guidelines for employees' use of social media and policies defining information parameters for employees who actively interact with past employees?

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)

39. Is the business aware of how cyber criminals and nefarious corporate competitors use social engineering tactics?

40. Does the business keep up with news on mobile device security vulnerabilities specific to the mobile devices used by the business?

41. Does the business use multifactor authentication (more than a password and logon) to access networks?

42. Does the business completely wipe data off ICT devices before disposing them?

43. Does the business forbid the use of USB devices at the workplace unless authorized by a supervisor?

44. Does the business have an effective digital defense plan in the event of a digital reputation crisis?

45. Does the business have an online corporate statement for quick release in the event of a digital reputation crisis?

46. Does the business have a prepared press release for immediate dissemination in the event of a digital reputation crisis?

47. Does the business have a video message for immediate dissemination in the event of a digital reputation crisis?

48. Does the business have a social media mention for immediate dissemination in the event of a digital reputation crisis?

49. Does the business have a formal e-mail statement for immediate dissemination in the event of a digital reputation crisis?

50. Does the business have a set of planned Tweets for immediate dissemination in the event of a digital reputation crisis?

51. Does the business have a micro-site or dark site that can be activated in the event of a digital reputation crisis?

52. Does the business know delaying a response to business complaints and online reputation attacks allows criticism to go "viral"?

53. Does the business know the longer business criticism goes unanswered, the more truthful it appears and the more defensive a response seems?

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)

54. Does the business know inaccurate rumors left unchallenged online can be highly problematic?

55. Is the business assessed as proficient at getting out the facts effectively in the event of a digital reputation attack?

56. Is the business aware that a disgruntled customer or ex-employee can cause havoc with the business's online reputation?

57. Does the business know that prompt and effective action is critical to protecting the digital reputation?

58. Does the business encrypt the hard drives to help protect vital data in case of theft or loss?

59. Does the business use pass codes for mobile devices as well as subscribed to remote wipe services?

60. Does the business document and itemize the entirety of what personal information is retained in digital files, mobile devices and computers?

61. Does the business monitor and track who sends sensitive personal information from the business, how often and the information disclosed?

62. Does the business monitor how online personal, financial & proprietary information is disseminated throughout the business network?

63. Does the business know the body of information that is collected at each entry point?

64. Does the business know where information is kept that is collected at each entry point (i.e. central computer database, individual laptops, disks or tapes?)

65. Does the business monitor how personally identifying information (i.e. social security numbers, credit card numbers, financial information) is stored?

66. Does the business shred and destroy customer credit card information unless it has a business need or relevant to fiscal recording procedures?

67. Does the business check the default settings of the software that reads customer credit card numbers and processes transactions?

68. Does the business have a written records retention policy to identify what information must be kept and how it is secured for easy presentation to related authorities?

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)

69. Does the business only use social security numbers for required and lawful purposes like reporting employee taxes?

70. Does the business refrain from using social security numbers as employee or customer identification numbers?

71. Does the business have a data security plan that includes physical & electronic security, employee training and the security practices of contractors and service providers?

72. Does the business identify the computers or servers where sensitive personal information is stored and where back up database information is funneled?

73. Does the business identify all connections to the computers and servers where sensitive information is stored?

74. Does the business assess the vulnerability of social networking site profiles representing the business for potential cyber-attacks?

75. Does the business refrain from storing sensitive customer data on computers with an Internet connection unless it is essential?

76. Does the business check the software vendors' websites regularly for alerts about newly released or identified vulnerabilities?

77. Does the business scan the computers on the network to identify and profile the operating system and open network services?

78. Does the business receive and transmit sensitive financial data using a Secure Sockets Layer (SSL) or another secure connection that protects the information in transit?

79. Does the business use password activated screen savers to lock employee computers after a period of inactivity?

80. Does the business lock out users who do not enter their correct password within a designated number of log-on attempts?

81. Does the business immediately change vendor-supplied default passwords to a more secure strong password when installing new software?

82. Does the business restrict the use of laptops to those employees who do not need them to perform their work tasks?

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)

83. Does the business require employees to store laptops in a secure place?

84. Does the business require employees to immediately notify a designated employee if there is a potential security breach?

85. Does the business investigate security incidents immediately and take steps to close off existing threats to personal information?

86. Does the business password protect all mobile devices that hold sensitive data and encrypt them effectively?

87. Does the business know how to securely back up all the mobile devices often?

88. Does the business monitor and inventory all portable electronic devices always?

89. Does the business turn off wireless services when they are not being used for business functions?

90. Does the business know exactly who, what, where & how it is connecting to always prioritizing network security?

91. Does the business keep mobile device security software current by having the latest mobile security software, web browsers and operating systems?

92. Does the business know what data (i.e. location, access to the social networks) on mobile devices an application can access before it is downloaded?

93. Does the business know how to disable the geotagging feature on mobile devices?

94. Does the business know about Wi-Fi hotspots and what types of business functions to limit?

95. Does the business know when banking and/or shopping using mobile devices to look for web addresses with "https://" or "shttp://"?

96. Is the business educated about and protected from credit card fraud?

97. Is the business educated about and protected from identity theft?

98. Is the business educated about DHL/UPS frauds?

99. Is the business educated about Escrow Services Fraud?

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)

100. Is the business educated about Internet Extortion?

101. Does the business cover the digital copiers used in its information security plan?

102. Does the business refrain from frequenting peer-to-peer networking sites?

103. Does the business refrain from clicking on links in an Instant Message (IM) and email message from unknown senders?

104. Does the business regularly review the list of applications authorized to access the Twitter account via the Twitter Settings Connections page?

105. Does the business preview short URL's before clicking on them when using Twitter?

106. Does the business refrain from sharing sensitive information on Twitter unless confident of whom is receiving the information?

107. When using Twitter, does the business know how to make a Twitter feed private when communicating among colleagues?

108. Is the business careful when using wireless hotspots at airports or hotels given there is no security at all on free wireless hotspots?

109. Does the business know sensitive data, such as passwords and account numbers, should never be stored on mobile devices?

110. Does the business have a policy requiring all mobile devices to wipe clean after a certain number of incorrect passwords?

CORRECT RESPONSES TO ALL IPI-B QUESTIONS A. Y__ (Yes, Agree, True)

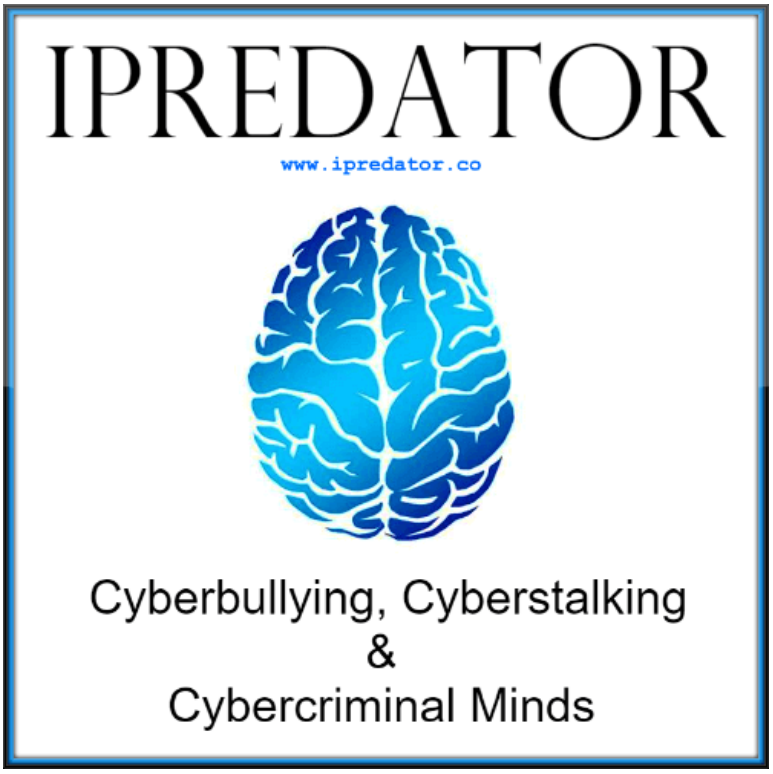
Yes Answers __ No Answers __ I Do Not Know__ Does Not Apply__

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