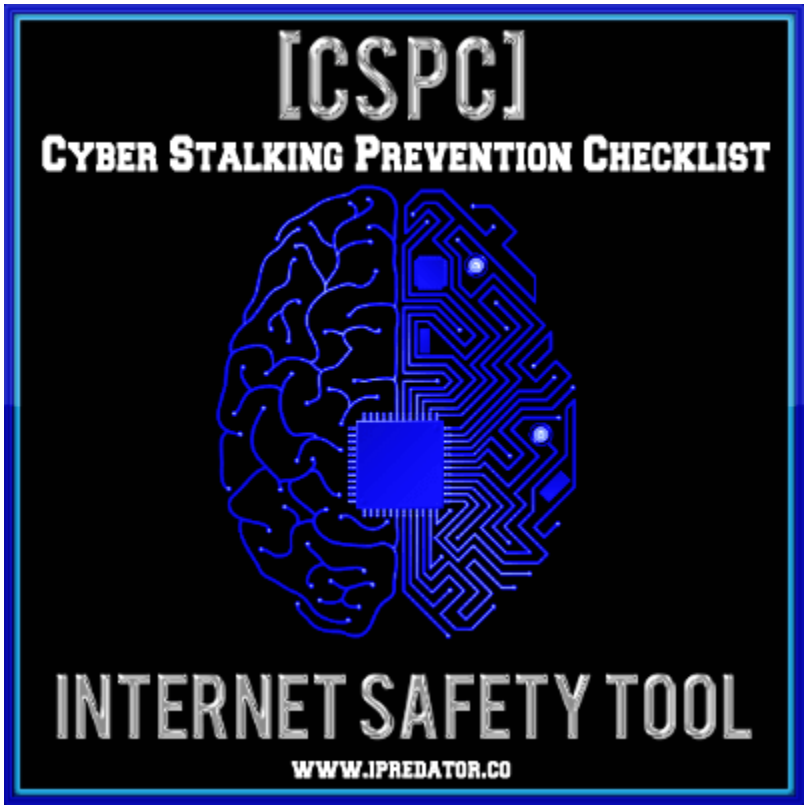
CSPC

Cyberstalking Prevention Checklist

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



Cyberstalking Prevention Checklist (CSPC)

The Cyberstalking Prevention Checklist is a 100-item data collection, diagnostic and educational tool designed to confirm the preparedness of an online user being cyberstalked and/or cyber harassed. The CSPC investigates personal and/or corporate vulnerability of being targeted, disparaged, harassed, monitored or infiltrated by cybercriminals, cyber terrorist, cyberstalkers, disgruntled ex-partners, disgruntled past employees/customers or nefarious corporate competitors.

Areas examined in the CSPC include online risk behaviors, identity theft potential, personal and financial information protection, ICT safety, cyber security and cyberstalking preparedness. The CSPC combines aspects of cyberstalking, cyber harassment and cyberbullying if the subject being queried is a minor.

The CSPC can also be used, as a data collection instrument to present to authorities if an online user is actively being cyberstalked or harassed. The CSPC has been designed with the knowledge that cyberstalking is both a method used by assailants and a typology of offender who engages in the behavior of cyberstalking. The CSPC also addresses the growth of mobile device technology and attempts by cyberstalkers to infiltrate their target's mobile devices.

CSPC DIRECTIONS

1. The time needed to complete the CSPC checklists 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 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.

CSPC

Cyberstalking Prevention Checklist

Note: Cyberstalkers attempt to target all social systems of a target and it is for this reason each statement in the CSPC includes the phrase "You". Cyberstalking prevention needs the teamwork of all social groups involved in the life of the potential target.

Subjects Gender: Male__ Female__
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. You ignore being "flamed" (provocative online communications).
2. You have a genderless screen name.
3. You post minimal personal information online.
4. You know your state cyberstalking, cyberbullying and cyber harassment laws.
5. You refrain from posting a home address online.
6. You password protect all ICT with secure passwords that are difficult to guess.
7. You continually change passwords and secret questions on all ICT accounts.
8. You are always suspicious of incoming emails, telephone calls or text messages that ask for personal identifying information.
9. You never gives out a Social Security Number or financial information to unknown online entities.
10. You refrain from teasing or threatening online users.
11. You regularly check the status of your credit reports regarding online transactions.
12. You have all internet enabled devices regularly checked for spyware.
13. You refrain from sharing contact information in e-mail, IM, text, Twitter and chat room messages.
14. You are extremely cautious about meeting online acquaintances in person.
15. You make sure your ISP and Internet Relay Chat (IRC) networks have an acceptable use policy prohibiting cyberstalking.
16. You know to log off and contact local law enforcement if a situation becomes physically threatening.
17. You know to save all communications for evidence if cyber attacked or harassed.
18. You know to keep records of contacts with internet system administrators and law enforcement if cyber attacked or harassed.
19. You know how to block or filter messages from a potential cyberstalker or harasser.
20. You know how to report an online assailant to an Internet Service Provider (ISP).
21. You know what to do if an online assailant posts felonious sex ads/images about you.
22. You know to contact the police and inform them in detail if cyberstalked or harassed.

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)

23. You are not afraid to act if cyberstalked or harassed.
24. You regularly review your "friends" and "buddy" lists and remove any connections that are not trusted ICT users.
25. You delete applications that are no longer used given they have access to personal information.
26. You know what to do if taunted by online strangers.
27. You know cyberstalkers may pose as their victim and attack others online.
28. You regularly conduct an internet search using your name and phone number.
29. You know what to do if receiving unwanted emails or text messages from an ex-partner, acquaintance or stranger.
30. You know what to do if receiving unsolicited threatening emails and/or death threats.
31. You do not post your home address online.
32. You know what to do if receiving extreme amounts of spam from an ex-partner, acquaintance or stranger.
33. You know what to do if sexually harassed via online posts, emails, phone or text messages.
34. You will not respond to an online user suspected of harassing you online.
35. You know what to do if you find your personal information without your consent posted by an ex-partner, acquaintance or stranger.
36. You know what to do if an email or cell phone account has been hacked.
37. You know what to do if subscribed to pornography and/or distasteful advertising sites without your consent.
38. You understand the difference between being cyberstalked and cyber harassed.
39. You know how to check if being tracked by GPS technology.
40. You know how to check if phone calls or messages are being intercepted.
41. You know what to do if being impersonated online.
42. You know what to do if being watched by hidden cameras and/or other forms of digital surveillance.
43. You know if being stalked or harassed by a stranger, there is a good chance it is an ex-partner, acquaintance or fan.
44. You know online assailants contact victim's family or employer.
45. You know online users who post personal information, when blogging, have higher rates of cyberstalking and harassment.
46. You know cyberstalkers and harassers follow their victim from site to site.
47. Email addresses, instant messaging usernames and links to personal homepages cannot be connected to you.
48. You know cyberstalkers may commit identity theft by opening or closing accounts, taking funds or charging purchases to your credit card.
49. You know a cyberstalker can be an obsessed lover or someone with a grudge due to a minor or imagined reason.

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. You know online assailants may pose as online friends asking innocuous questions they will use to guess your passwords.
51. You know that most cyberstalking and harassment involves someone you know or recently interacted with.
52. You never have and never will share sexually themed content via internet enabled devices.
53. You know an online assailant can be an egotistic aggressor who wants to show-off to their peers.
54. You know to avoid announcing your physical location via status updates of GPS-enabled applications.
55. You know changing *"Internet Service Providers"* and reporting cyber-attack events is recommended to help stop cyberstalking and harassment
56. You know it is recommended to contact your local FBI Computer Crimes Unit if physically threatened online.
57. You know an unattended logged in computer should be turned off.
58. You know to contact the proper authorities if someone sends you threatening, lewd or harassing emails
59. You have a plan of action if an online assailant or stalker showed up to your job.
60. You know what to do if someone is posting messages to online bulletin boards and discussion groups with your financial or personal information.
61. You know online assailants may impersonate their victim and post lewd or controversial information.
62. You know what to do if signed up for many online mailing lists and services without your consent.
63. You know your state cyberstalking and cyber harassment laws.
64. You refrain from using gender specific or provocative screen names.
65. You refrain from flirting or arguing online with both known and unknown ICT users.
66. You avoid posting personal information on all social media accounts.
67. You know to warn friends and acquaintances not to post your personal or contact information and location.
68. You know not to post photographs of your home that might indicate its location by showing a house number or an identifying landmark in the background.
69. You know to use caution when joining online organizations, groups or "fan pages" and never publicly RSVP to events online.
70. You know to use caution when connecting a mobile device to a social networking account.
71. You know to avoid posting information about your current or future locations, such as a review of a restaurant you have posted near your home.
72. You know to only post information that would not expose you to harm if a cyberstalker or harasser should read it.

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)

73. You know that cyberstalking can be orchestrated by the assailant, friends and associates working as a team in their attacks.
74. You have a general idea about who is an *"Intimacy Seeker"* cyberstalker is.
75. You know have an emergency cash fund in case an online assailant steals your money.
76. You know online users are particularly susceptible to cyberstalking and harassment if video blogging (vlogging).
77. You know about and/or signed up for your state's address confidentiality program.
78. You know how to sign up for an unpublished or unlisted phone number.
79. You know about and/or signed up for *"Caller ID Complete Blocking"* also called *"Per Line Blocking"*.
80. You know where to buy a pre-paid cellular phone with cash.
81. You know when a phone is powered off completely, the police or a telecommunications carrier cannot track its location.
82. You know to avoid calling toll-free number services because your phone number can be captured by a service called *"Automatic Number Identification"*.
83. You know how to have your name removed from *"Reverse Directories".*
84. You know to never use your residential address for anything that is mailed to you by an unknown entity.
85. You know to never use your middle initial online, since middle initials are often used to differentiate people with common names.
86. You know when conducting business with a government agency to only fill in the required pieces of information.
87. You avoid clicking on redirect links from users you do not know.
88. You know not to put your name on the list of tenants on the front of your apartment building.
89. All your screen names are gender and age neutral.
90. You know to keep notes and document if stalked or harassed for evidence.
91. You know about *"Sextortion"* and how it is used by online assailants.
92. You would be extremely cautious about meeting an online stranger in person.
93. If you buy a domain name for a website/blog, you will register it privately, so your personal information is not publicly available.
94. You know how to contact court to start a "*Restraining Order*" or "*Order of Protection*".
95. You know how to set up alerts with search engines to alert you of content being disseminated about you.
96. You know how to deactivate all social media accounts if concerned about being cyberstalked or harassed.
97. You know how to access and control the privacy settings in your social media accounts.
98. You know to avoid clicking on redirect links from users you do not trust.
99. You practice *"Digital Citizenship*" and do not engage in *"Flaming".*

100. You refrain from posting or sharing personal information online that is provocative, violent, sexually suggestive or age inappropriate.

Yes Answers___No Answers___I Do Not Know___Does Not Apply___

Yes Answers___ + Does Not Apply___ = CSPC Score__

CORRECT ANSWER FOR EACH CHECKLIST STATEMENT IS Y__ (Yes, Agree, True)

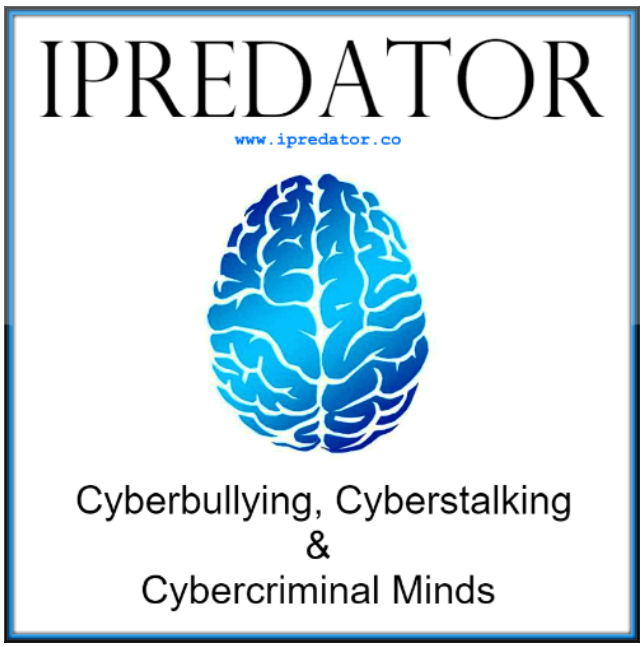
Note: The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. *"I Do Not Know"* & *"No"* responses should be addressed at once with a plan of action.

(link for web page scoring key)

Internet Safety Tool Scoring Keys Page: https://www.ipredator.co/scoring-keys/

Given the rapid expansion and advancements in ICT, it is recommended to complete the CSPC 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.

Although obtaining a high score indicates a minimal probability of a damaging cyber-attack, it is still always crucial to be alert and prepared to defend against iPredators as they change their tactics paralleling advancements in technology. Cyberspace is a non-physical abstract electronic universe. The toll it can take on vulnerable and/or ignorant ICT users are very real and can range from frustrating to deadly.



IISC SCORE DEFINITION

IISC Score: Upon completion of any of the IISC assessments, the respondent will have a final score ranging from 0-75, 0-100 or 0-300 depending on the IISC assessment. In this formula, the score represents the risk potential and vulnerability of the ICT user, the business or the subject being queried from being targeted by a cyberbully, cyberstalker, cybercriminal, nefarious corporate competitor or online sexual predator. Whether taken one time or on multiple occasions, the goal is to finish with a score in the top 10% of all the IISC assessments.

IISC SCORING KEY

Cyberstalking Prevention Checklist
CSPC

Note: Just as all the IISC tools, it is recommended to take the CSPC on a quarterly basis. The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. "IDK" & wrong responses should be addressed at once with a structured plan of action.

If and/or when you score a 90 or higher, you are skilled in internet safety strategies and understand the dangers that lurk in cyberspace. You, the business being assessed or the subject you are assessing are encouraged to educate others in your community.

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

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

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

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

Score: (56-78)
Category: Possible Cyberstalking Target and Moderate Vulnerability.
Risk Potential: Moderate.
iPredator Involvement: Involvement Possible.
Intervention Plan: Increase iPredator Protection & Prevention Strategies.
Level of Urgency: Immediate Attention Suggested.

Score: (79-89)
Category: Skilled Cyberstalking Protection and Low Vulnerability.
Risk Potential: Mild.
iPredator Involvement: Possible, but Unlikely.
Intervention Plan: Continue iPredator Protection & Prevention Strategies.
Level of Urgency: Not Urgent, Important to Address if Score Below 85.

Score: (90-100)
Category: Advanced Cyberstalking Protection and Minimal Vulnerability.
Risk Potential: Minimal.
iPredator Involvement: Unlikely.
Intervention Plan: Consider Educating Others.
Level of Urgency: 0%, All iPredator Issues Addressed.

Michael Nuccitelli, Psy.D.

Michael Nuccitelli, Psy.D. is a NYS licensed psychologist, cyberpsychology researcher and online safety educator. In 2009, Dr. Nuccitelli finalized his dark side of cyberspace concept called iPredator. Since 2010, he has advised those seeking information about cyberbullying, cyberstalking, cybercriminal minds, internet addiction and his Dark Psychology concept. By day Dr. Nuccitelli is a practicing psychologist, clinical supervisor and owner of MN Psychological Services, PLLC. After work and on the weekends, he volunteers helping online users who have been cyber-attacked. Dr. Nuccitelli's is always available to interested partied and the media at no cost. The iPredator website and everything created by Dr. Nuccitelli is educational, free and public domain.