AISC

Adult Internet Safety Checklist

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

Adult Internet Safety Checklist (AISC)

The Adult Internet Safety Checklist (AISC) is a 100-item checklist designed for an adult online user to verify their internet safety practices and cyber-attack awareness. The AISC was also created to investigate an adult's preparedness of being taunted, criminalized and/or victimized by iPredators. As a data collection tool, the AISC can be used to investigate an online user's efforts to reduce their probability of being targeted, disparaged, stolen from or infiltrated by cybercriminals, cyberstalkers, online sexual predators or those engaged in digital reputation disparagement.

The AISC enables the respondent to examine their online and ICT interactions in relationship to iPredators and the weaknesses they can focus upon to reduce the potential of successfully being cyber attacked. With the rapid growth and expansion of information technology, all online users must give time and effort employing cyber security and digital reputation management. The AISC also addresses the growth of mobile device technology and tries by cyber criminals to infiltrate their target mobile devices.

AISC DIRECTIONS

1. The time needed to complete the AISC 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 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 issue information. ICT stresses the role of unified communications and the integration of telecommunications, which enable users to create access, store, send 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.

AISC

Subject's Gender: Male__ Female__
Age: (18-32) __ (33-45) __ (46-54) __ (55-70) __ (71+) __
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. Your email addresses, instant messaging usernames and links to personal homepages cannot be connected to your home address or identity.
2. You do not share your physical location via status updates on GPS-enabled applications.
3. You never leave a logged in internet enabled device unattended for extended periods.
4. You know what *"Digital Footprint"* means and actively check it.
5. You have not shared sensitive information to an ex-loved one online.
6. You are cautious about what you share, exchange and post online.
7. You protect your private content from being downloaded or shared by strangers.
8. You keep separate your online personal life from work as a digital reputation control measure.
9. You know what *"Digital Reputation"* means and maintain a positive online presence.
10. You know your images and videos can remain online for years.
11. You do not have a mobile device that has embarrassing and/or sensitive information.
12. You are careful about posting personal information and know why it is important to internet safety.
13. You refrain from "sexting" and know it is criminal if the content involves a minor.
14. You have not shared confidential information to an online associate that involves money.
15. You know how to create and keep a respectable online presence.
16. You know your images and videos can remain in cyberspace for years.
17. You have a general understanding of what *"Identify Threats"* means.
18. You know *"Sexting"* content can be shared without your consent.
19. You do not have sexual conversations with online strangers.
20. You review the privacy and security settings before joining social media sites.
21. You do not call, text message or chat with online strangers.
22. You have not been contacted by an online stranger and kept it a secret from others.
23. You know what *"Sextortion"* means and how to avoid being blackmailed.
24. You do not habitually spend money on internet sex sites.
25. You do not go online when highly intoxicated.

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. You always choose strong passwords.
27. You meet online strangers in public for the first meeting.
28. You watch your online financial transactions for any fraudulent activity.
29. Your internet security software is up to date on all devices.
30. You do not take part in anonymous video or chat room sites.
31. You do not engage in online activities that are discouraged by internet safety sources.
32. You know to log out of a website or online conversation if feeling uncomfortable.
33. You do not engage in online activities you do not want a loved one to know about.
34. You would not meet an online stranger offline without a loved one knowing.
35. You know what *"Social Engineering"* attacks are and how to prevent them.
36. You keep up with news about mobile device security vulnerabilities.
37. You share your passwords with no one.
38. You never open attachments or click on links from unknown sources.
39. Your mobile device has a passcode, PIN or fingerprint lock if lost or stolen.
40. You shut off your computer(s) and mobile devices when not using them.
41. You are aware iPredators may create online profiles pretending to be someone you consider attractive and/or intriguing.
42. You regularly check for new cybercrime protection apps, products and services.
43. You have strong passwords with more than five characters and have different passwords for different accounts.
44. You only download apps from trustworthy sources
45. You do not use social media to announce time spent away from home.
46. You always look for the *"locked"* icon at e-commerce sites.
47. You do not retaliate to negative online information being disseminated about you.
48. You never respond to unknown emails that ask for personal information.
49. You know how to prevent *"Internet Fraud"* and *"Identity Theft"*.
50. You do not connect your mobile device to public or unsecure WiFi.
51. You know how to encrypt your hard drives in case of theft or loss.
52. You check to confirm that your operating system software is up-to-date.
53. You know what personal and financial information you have stored in your devices.
54. You watch who sends sensitive personal information from your home and/or business.
55. You do not overshare personal information on social media.
56. You rarely misplace your mobile devices and know what to do if they are lost or stolen.
57. You do not use the same password for multiple accounts.

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)

58. You are aware iPredators use attention, affection and gifts to seduce online users.
59. You know how to disable the geotagging feature on your mobile devices.
60. You have not threatened, embarrassed, or teased another online user.
61. You periodically remove apps that you no longer need.
62. You check active online accounts and remove unused accounts.
63. You have a reliable backup of all the data on your mobile devices.
64. You know how to protect yourself against phishing schemes.
65. You are familiar with "*Ransomware*" and know what to do if cyber-attacked.
66. You would never post your contact information on high-risk websites (i.e. extremist, racist, violent).
67. You are aware iPredators target online users by using kindness and understanding.
68. You never share your social security number online.
69. You do not engage in unnecessary arguments with internet trolls.
70. You know GPS location services allow anyone to know your exact location at any given time.
71. You disable browser autofill and manually input credit card information.
72. You only make online purchases from "SSL" secure sites.
73. You know about peer-to-peer networks and how they can expose your devices.
74. You are honest about your online activities with loved ones.
75. You are suspicious if online associates encourage you to be deceptive.
76. You are familiar with bot software, spyware, keystroke loggers and viruses.
77. You have emergency contact numbers stored in your mobile device.
78. You do not add online strangers to your "buddy" and "friends" lists.
79. Your social media profiles do not publicly display when you are not at home.
80. You do not send sensitive information such as credit card numbers by email.
81. You verify ecommerce websites are secure before giving your credit card information.
82. You are mindful that you only download legal files, music and videos.
83. You do not feel more comfortable online than spending time with loved ones off-line.
84. You do not save your banking app ID on your device.
85. You have not been told by loved ones that you are isolating online.
86. You are not spending more time online due to home, school or work stress.
87. You read and understand refund, return and guarantee policies when shopping online.
88. You do not text message or view/share online content when driving.
89. You have not been less productive in school, work or major responsibilities due to your online activities.
90. You disable WiFi and Bluetooth on your devices when not in use.
91. You know that public wireless networks are not secure and careful about what you share.
92. You are 100% sure that antivirus software is up-to-date on all your devices.
93. You do not engage in cyberstalking or cyber harassment

94. You do not "Jailbreak" or "Root" on your mobile devices.
95. You would never share or download sexual content involving minors.
96. You are aware of *"Flaming"* and do not take part in online arguments.
97. You intermittently research new types of cybercrime.
98. Loved ones have not confronted you about being internet addicted.
99. You have not been confronted about time spent online gaming.
100. You occasionally research "*Social Media Safety*" and/or "*Internet Safety*".

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__

Yes Answers__ + Does Not Apply__ = AISC Score__

CORRECT RESPONSE TO ALL STATEMENTS: Y__ (Yes, Agree, True)

Note: The goal for best internet safety & cyber security functioning is to score a 90 or higher. "*I Do Not Know*" & "*No*" responses should be addressed at once with a plan of action. Although obtaining a score of 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 continues to expand, it will become increasingly important to manage and check cyber-attack prevention 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 the AISC on a quarterly basis and more often if an iPredator is suspected of engaging in a possible cyber-attack. To achieve best cybercrime, cyber-attack and/or cyber assault prevention, the goal is to score in the upper 10%-15% of all the IISC assessments. "I Do Not Know" & wrong responses to IISC items should be addressed at once with a proactive plan of action. Although cyberspace is a non-physical abstract electronic universe, the toll it can take on vulnerable and/or ignorant ICT users can 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 stands for 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.

IPREDATOR

IISC SCORING KEY

Adult Internet Safety Checklist
AISC

Note: Just as all the IISC tools, it is recommended to take the AISC on a quarterly basis. The goal for best 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. Although obtaining a score of 90 or higher indicates a minimal probability of a successful cyber-attack and active internet safety protection, it is still always crucial to be alert and prepared to defend against iPredators.

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 iPredator 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 iPredator 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 iPredator 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 iPredator 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 iPredator 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 ICT 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 ICT 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.