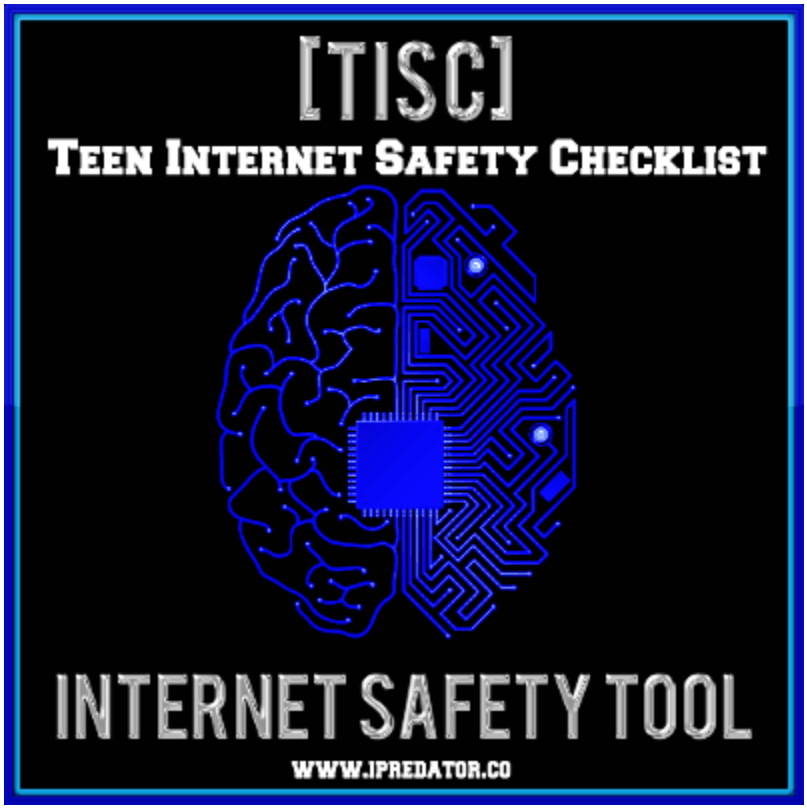
TISC

Teen Internet Safety Checklist

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



Teen Internet Safety Checklist (TISC)

The Teen Internet Safety Checklist (TISC) is a 100-item education, assessment and data collection tool designed for teachers, educators and pediatric professionals related to pre-pubescent and adolescent internet safety and responsible Information and Communications Technology (ICT) usage. The TISC is formatted in a way allowing the adolescent, an adult or both parties to complete the checklist. The TISC queries and explores areas developmentally relevant to an early adolescent, adolescent and young adult, ages 11-18.

These areas include sexuality, intimate partnerships and perceived peer group acceptance in relationship to their internet safety practices. The goal of the TISC is to educate children on their vulnerability and risk potential of being targeted by an iPredator engaged in cybercrime, cyberstalking, cyber harassment, cyberbullying or trolling for a target to sexually victimize.

In addition to a data collection and educational tool, the TISC has been designed to allow teachers, educators and pediatric professionals to interview, collect data and engage in a dialogue with children and teens regarding their online practices. The TISC also addresses the growth of mobile device technology and attempts by iPredators to infiltrate their target's mobile devices.

TISC CHECKLIST DIRECTIONS

1. The time required to complete the TISC checklists 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.

Teen Internet Safety Checklist

(TISC)

Gender: Male__ Female__
Age: (11-14) __ (15-16) __ (17-18) __
Average Daily Online Activity: 0-1Hours__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. If someone has been verbally abusive towards you online, you will tell your parents or a trusted adult.
2. You have not been harassed or teased someone online and kept it a secret from your parents or a trusted adult.
3. You have not been "flamed" and kept it a secret from your parents or a trusted adult.
4. You have not sent, posted or received mean messages about others and did not tell anyone.
5. You have not had an online relationship go bad and you began teasing and/or harassing them.
6. You have not had secrets spread by others online and kept it a secret from your parents or a trusted adult.
7. You know what to do if you or a friend is being teased, harassed or cyber bullied.
8. You are careful about what you disclose to others online.
9. You always protect your images and videos from online strangers from viewing them.
10. You have not been harassed or teased online on the grounds of your race, religion, gender, sexuality or physical look.
11. You have not and would not retaliate to negative online information being spread about you.
12. You are careful about posting your personal information online and know why it is important related to your "*Digital Reputation*".
13. You know what "*Digital Footprint*" means or how posting your personal information online can hurt your reputation.
14. You have not shared confidential information to a now ex-friend online and concerned about what they will do.
15. You work to have a positive "*Digital Reputation*" or know how to create a positive "*Digital Reputation*".
16. You know the images and videos you post online can remain in cyberspace for years.
17. You know sensitive and/or sexual information you share online may be impossible to delete.

18. You know "*Sexting*" involving you or friends can be shared with others without your consent.
19. You know not to have sexual conversations with someone you met online.
20. You always review the privacy and security settings at social media sites you have joined.
21. You know not to call, text message or chat with online strangers.
22. You have not been contacted by an online stranger and kept it a secret from loved ones.
23. You have never met someone in person you met online and did not tell loved ones.
24. You know to never respond to online strangers who ask for money.
25. You do not have a social media profile with personal information available to the public.

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 do not have a mobile device with information that is embarrassing, sexual or secret.
27. You know about iPredators, cyber harassment and cybercrime.
28. You know iPredators target children, teens and adults using kindness and understanding.
29. You know how cybercriminals engage in identity theft and online fraud.
30. You know iPredators will encourage you and your friends to add them to their buddy lists.
31. You give your mobile device passwords to the adults you trust implicitly.
32. You know how to prevent unwanted access to your mobile devices or cell phone.
33. You are knowledgeable about the dangers of GPS location services.
34. You know GPS location services allows anyone to know your exact location at any given time.
35. You are aware iPredators use attention, affection and gifts to seduce children, teens and adults online.
36. You know iPredators may create online profiles pretending to be someone you think is attractive and/or intriguing.
37. You know what peer-to-peer networks are and how they can expose your computer and network to iPredators.
38. You know most children and adults are victimized by family members, family friends and trusted peers.
39. You know to be suspicious of anyone online who encourages you to be defiant, deceptive or lie to loved ones or teachers.
40. You know iPredators look for children, teens and adults who will access their phones or the internet during late night hours.
41. You spend time learning mobile device safety.

42. You know how to install security on your mobile devices.
43. You know and comply with school or work policies regarding mobile device usage.
44. You have downloaded and installed antivirus software on your mobile devices.
45. You always make sure to set and check your privacy settings.
46. You know it is beneficial to have multiple passwords and to change them often.
47. You do not visit "private" chat rooms or questionable websites and keep it a secret from loved ones.
48. You are familiar with bot software, spyware, keystroke loggers and viruses.
49. You know that iPredators frequent social media sites like Facebook, Instagram and chat rooms.
50. You are prepared if friends introduce you to questionable and high-risk websites.

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. You know that you can accidentally disclose your phone number by "*Caller ID*" to online strangers.
52. You know what to do if you are exposed to sites dealing with hatred, violence, racism or graphic content.
53. You never post or share your home or cell phone numbers with people you have met online.
54. You do not spend large periods of time online involved with social networking sites.
55. You always log off when not using instant messaging or your email accounts.
56. You know about the dangers of disclosing your personal and/or contact information online.
57. Your user accounts or profile names do not include your full or partial real name.
58. You do not visit anonymous chat room and video chat sites.
59. You always refrain from sharing your social security number online.
60. You do not click on links or attachments in your email from unknown senders.
61. Your school, college or job's website is password protected so online strangers cannot access your images if posted there.
62. You never give your credit card information online unless you are 100% sure the payee is trustworthy.
63. You know how to recognize identity thieves that pretend to be a trusted organization.
64. You know to never send sensitive information, such as credit card numbers, by email.
65. You only download legal files, music and videos.
66. You do not spend less offline time with friends and family and more time online.
67. You have a personal cutoff time for being online if it is not school or work related.

68. You would talk to loved ones or a trusted adult if you felt depressed, distressed or angry about something that happened online.
69. When you have thoughts or questions about sexuality, you will never ask someone you met online.
70. You do not allow others, you do not know, to join your "friends" or "buddy" lists.
71. You are not less interested in your favorite offline activities.
72. Loved ones, friends or coworkers have not recently said you have changed or isolating more.
73. You will always speak to your parents or a trusted adult if you feel stressed or anxious.
74. You have not been less attentive, less productive or falling behind in school, work because of your time spent online.
75. You do not have a social media account you access more than 15 times a day.

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)

76. You always make sure to set and check your privacy settings often.
77. You do not allow others, you do not know, to join your "friends" or "buddy" lists because it will make you look more popular.
78. You always limit who can view your profile on your social media accounts.
79. You discourage your friends from having social media profiles with information available to the public.
80. You never share private and personal details on your social media profiles.
81. You will always review the privacy and security settings before joining a social media site.
82. You would not disclose your phone number, address or images to an online stranger you think is attractive.
83. In chat rooms, you always use a nickname that is different from your screen name.
84. You know to always decline meeting someone you met online even if you think they are attractive.
85. If your online identity is or was different from your real-world identity, you always still practice internet safety.
86. In your social media accounts, your privacy settings are set to "friends only".
87. You know to never share or post inappropriate or sexually provocative pictures online.
88. You know what to do if a friend wants you to post inappropriate or sexually provocative comments about another peer.
89. You know to never share or post inappropriate or sexually provocative comments in chat rooms.
90. You and your close friends do not engage in sexting.

91. If you get an angry online message, you always wait and calm down before responding or do not respond at all.
92. You know to never post, share or distribute copyrighted images, songs, or files.
93. You are familiar with the cybercrime called "*Sextortion*".
94. You always think about the consequences before posting or sharing sensitive or personal information online.
95. You always talk to your parents or a trusted adult before you open an email attachment or download software.
96. You would talk to your parents or a trusted adult before visiting websites, chat rooms or blogs that are considered offensive.
97. If you were planning on meeting somebody you met online, you would bring a friend or your parents to the first meeting.
98. If you get suspicious e-mails, files or images from online strangers, you delete them immediately.
99. You are cautious about posting information that could reveal your true identify and home location.
100. Even if you thought you were 100% positive, you still would not flirt, contact or meet anyone you met online without first telling your parents or a trusted adult.

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__ = TISC Score__

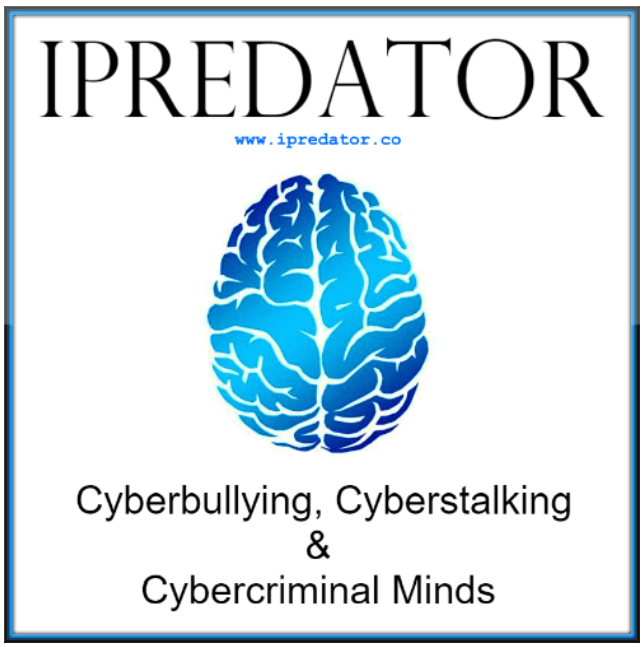
ALL CORRECT RESPONSES ARE A. Y__ (Yes, Agree, True)

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 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.

(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 TISC 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 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

Teen Internet Safety Checklist
TISC

Note: Just as all the IISC tools, it is recommended to take the TISC 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 immediately 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 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 iPredator 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 iPredator 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.