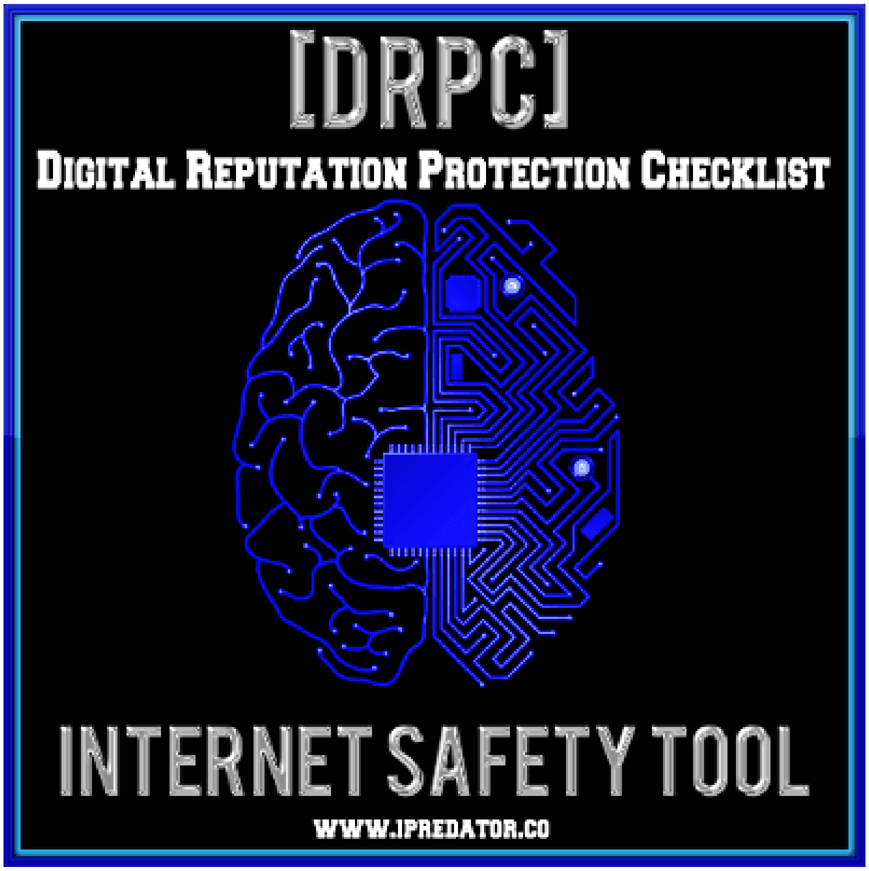
DRPC

Digital Reputation Protection Checklist

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



Digital Reputation Protection Checklist (DRPC)

The Digital Reputation Protection Checklist is a 100-item checklist designed for an online user and/or their business to monitor, protect and manage their digital reputation. Digital Reputation is a term used to describe the reputation of an online user or business that is disseminated online, created and sustained by peers, school, work associates, loved ones, acquaintances, consumers, competitors, adversaries, online strangers and online assailants. This information can be positive or negative and vital to the success, growth and health of an online users.

The DRPC is a data collection & assessment tool that investigates a business's vulnerability of being targeted, disparaged, slandered, stolen from or infiltrated by cyber criminals, disgruntled past employees, angry customers or nefarious corporate competitors. The DRPC focuses on the online user and the business's cyber-security breach potential, digital reputation acumen and ability to successfully institute online reputation prevention and protection strategies.

DRPC DIRECTIONS

1. The time needed to complete the DRPC 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 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.

DRPC

Digital Reputation Protection Checklist

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 monitor and evaluate your digital reputation weekly.
2. I practice *"Digital Citizenship"*.
3. You never post or share content online when angry or frustrated.
4. You regularly wipe cookie and search history caches.
5. There is no personal and financial information stored on internet enabled devices.
6. You actively maintains an up-to-date online presence by posting quality content.
7. You do not disseminate highly controversial or provocative online content.
8. You have segmented your online identity into personal and work themed personas.
9. You cannot be called an extremist or rigid ideologue by viewing your online content.
10. I have not been accused of being an internet troll more than twice.
11. You have segmented your personal life from your work persona and your social media persona.
12. You consistently update, monitor and manage a blog or website.
13. You consistently make sure to link to reputable sources and create content on a regular basis.
14. You consistently post content related to your business, hobbies or educational background.
15. You are familiar with the concepts and applications of *"Search Engine Optimization (SEO)"*, *"Search Engine Marketing (SEM)"* & *"Social Media Optimization (SMO)"*.
16. You have a prepared and ready digital reputation damage plan.
17. I have never compiled, shared or disseminated sexual content involving minors.
18. You conduct regular *"Advanced Google Searches"* using your name or business name.
19. You are familiar with the cybercrime called *"Sextortion"*.
20. I do not engage in *"Sexting".*
21. I regularly conduct image searches connected to my name.
22. You are familiar with and actively practice *"Digital Citizenship"*.
23. I fully understand the potential consequences of posting inappropriate material about my adversaries and competitors.
24. I have not posted images of myself or my business that I would not want online strangers to view.
25. You have access to legal representation if needed to take legal action for defamation and character assassination.
26. I understand the difference between *"Slander"* and *"Libel".*
27. You know *"Terms of Use"* for the social networking sites you have joined.

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)

28. You never click on links or open attachments in emails from online strangers.
29. You what action to take if being cyber harassed or threatened.
30. You delete or close unused social media accounts.
31. You work to maintain a strong online presence that displays your command of social media.
32. You actively practice *"Netiquette".*
33. You untag yourself from non-flattering social media photos and status updates.
34. Your business or employer have social media policies that must be adhered to by all employees.
35. I have never been accused of Spamming" on more than two occasions.
36. You have researched, compiled and created reputation management strategies for all potential information damaging scenarios.
37. Your online associates and loved ones understand the importance of not sharing your personal information.
38. You actively address and design efficient digital reputation management strategies that are effective, industry related and innovative.
39. You have not and would not discuss sexual themed content online.
40. You know how to handle internet trolls effectively.
41. I am extra careful what I share online if I have been drinking alcohol or using drugs.
42. The content you share online is always culturally sensitive.
43. Related to your business or profession, you understand the consequences of multiple negative reviews.
44. You understand what *"Character Assassination"* means and how to prevent it.
45. You regularly review the first 30-50 results of Google when searching for key phrases that relate to you, your business or your brands.
46. You manage your online presence by making frequent, relevant and consistent profile updates.
47. I have not been accused of cyberbullying or online workplace bullying.
48. You know about and prepared for *"Social Engineering"* attacks.
49. You have an effective digital defense plan in the event of a digital reputation crisis.
50. You have an online corporate/professional statement in the event of a digital reputation crisis.
51. You have not found your name or business name with negative reviews in review sites.
52. You know that delaying a response to complaints allows criticism to spread virally.
53. You know the longer criticism goes unanswered, the more truthful it appears and the more defensive a response seems.
54. You know inaccurate rumors left unchallenged can be highly problematic.

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)

55. You are effective at getting out the facts in the event of a digital reputation attack.
56. You that a disgruntled customer, ex-employee or ex-partner can cause havoc with your reputation.
57. You know that prompt and effective action is critical to protecting digital reputation.
58. I have never threatened an online user with physical harm.
59. You are familiar with the expression *"Don't Feed the Trolls"*.
60. You have a website or blog with quality content that uses your name or business as the domain name.
61. You are diligent in working to be a respected online user.
62. You post instructive and engaging content weekly.
63. You have a strategy to effectively contain a negative *"Viral Reputation"*.
64. You create 100% original content for all your keyword rich sites for improved ranking.
65. I have not been accused of cyberstalking or harassing an ex-partner or associate more than twice.
66. You have researched, purchased and secured all website variations for your name or company.
67. You and your business resist arguing about politics or religion online.
68. In the face of an online reputation attack, you have original content to post daily, weekly or monthly to your website or blog.
69. You react quickly and politely to online criticism.
70. You have press releases for immediate distribution to keep your brand(s) in the news in case of an unexpected reputation attack.
71. You know how to use online criticism to create and disseminate a powerful response.
72. You know the difference between bragging and sharing your attributes in a decent way.
73. You know that YouTube and videos are effective ways to maintain or repair an online reputation.
74. In most cases, you know to never comment on negative content about you or your business.
75. You are skilled in the identification and tactics used by internet trolls.
76. You have a high quality linking strategy to your website, blog or social media accounts.
77. You are cautious when posting content about your competitors or adversaries.
78. I knows what "*Digital Footprint*" means and its importance to digital reputation management.
79. You do not participate in online debates involving highly provocative issues.
80. You constantly add content to platforms specific for your industry or hobby.
81. You regularly compliment online users when they post high quality content.

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)

82. You know images and videos can remain in cyberspace for years.
83. You know information shared online may be impossible to delete or hide.
84. You know how to properly title your images using your name and/or business name.
85. You intermittently respectfully comment in online communities and forums.
86. You have Google+ account that you update daily.
87. You know that high quality educational images and videos can be reposted multiple times.
88. You know your offline stress levels can impact your online responses.
89. You take steps to ensure information about you or your business is accurate and factual.
90. You are willing to apologize online if you are wrong or inaccurate.
91. You are willing to participate in educational internet radio and other forms of multimedia.
92. You know that internet trolls try to provoke their targets into making profane and graphic rebuttals
93. I have never been accused of lying or exaggerating about my accomplishments more than two times.
94. You understand that a positive online reputation requires time, effort and sometimes money.
95. You are prepared to take legal action if someone portrays you or your business inaccurately online.
96. You research trends in new ways online assailants engage in character assassination.
97. You have *"Google Alerts"* set up using your name or business name.
98. You actively reach out to satisfied customers and positive online allies
99. You promptly respond to both positive and negative reviews.
100. I leverage my coworkers and loved ones to be reputation ambassadors in social media

Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Yes Answers__ + Does Not Apply__ = DRPC Score__

CORRECT RESPONSE TO EACH CHECKLIST ITEM IS Y__ (Yes, Agree, True)

IPREDATOR

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 DRPC 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% on 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

Digital Reputation Protection Checklist
DRPC

Note: Just as all the IISC tools, it is recommended to take the DRPC 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 Reputation 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 Reputation 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 Reputation 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 Reputation 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 Reputation 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 Reputation 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 Reputation 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.