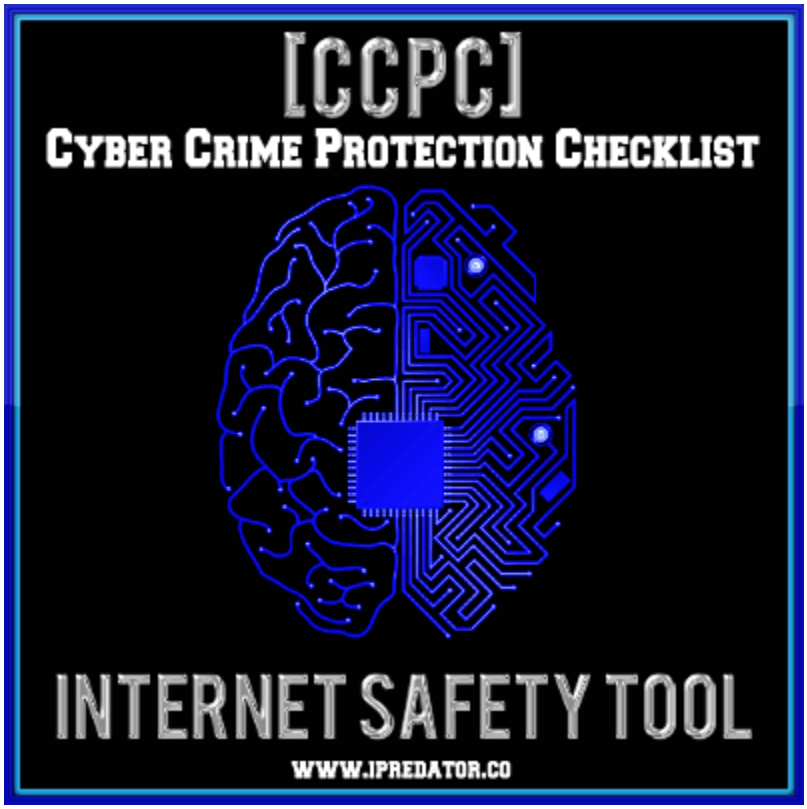
CCPC

Cybercrime Protection Checklist

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



Cybercrime Protection Checklist (CCPC)

The Cybercrime Protection Checklist is a 100-item checklist designed for an Information and Communications Technology user, their loved ones or business to assess their vulnerability and risk potential of being targeted. The CCPC assesses the probability of being disparaged, stolen from or infiltrated by iPredators, cyber terrorist or nefarious corporate competitors engaged in cybercriminal and/or cyber warfare activities.

The CCPC also investigates personal and/or corporate vulnerability of being targeted, disparaged, slandered, stolen from or infiltrated by cyber criminals, disgruntled past employees/customers or nefarious corporate competitors. Areas examined in the CCPC include identity theft potential, personal and financial information protection, ICT safety, cyber security and security breach potential.

It is recommended to complete the CCPC on a quarterly basis and more often if known adversaries, corporate competitors or malevolent entities are suspected of engaging in possible cyber-attacks or personal/corporate disparagement. It is also strongly encouraged for businesses, professional & organizational structures and public figures to make sure their colleagues, associates and sub-contractors practice the same level of cybercrime protection. The CCPC also addresses the growth of mobile device technology and attempts by cyber criminals to infiltrate their target's mobile devices.

CCPC DIRECTIONS

1. The time required to complete the CCPC 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 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.

CCPC

Cybercrime Protection Checklist

Note: The term "business" in the CCPC 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. All ICT is safe from hackers and checked regularly for updates.
2. All ICT is safe from viruses and checked regularly for updates.
3. All ICT is safe from malware and checked regularly for updates.
4. All ICT is safe from a mobile device cyber security breach and checked regularly for updates.
5. You or the business have a formal or informal written internet security plan.
6. You or the business takes part in internet safety training or education.
7. All ICT gets automatic software and security updates.
8. You or the business regularly inspects what information you have and what is needed to protect it.
9. You or the business regularly inspects how to store and protect data on mobile devices.
10. You or the business do not share personal information on social networking sites.
11. You or the business regularly assesses what new privacy settings you may need at social networking sites.
12. You or the business are aware of the information you put online and the potential value to a cybercriminal or cyber terrorist.
13. You or the business review bank and credit card statements regularly.
14. You or the business is aware of what websites and social networking sites are being visited during downtime at the workplace or at your home.
15. You or the business are educated on safe online practices.
16. You or the business have up to date antivirus software that monitors viruses, worms and other types of malicious programs.
17. You or the business are prepared to combat the latest cyber threats.
18. You or the business are safe from a loss of data and checked regularly.
19. You or the business are safe from loss of customer or personal information and regularly inspected.
20. You or the business have guidelines or rules on how long to store online documents.
21. You or the business have social networking site guidelines on what is permissible to share online.

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)

22. You or the business have social networking site guidelines on how to safeguard private, personal and/or financial information.
23. You or the business are educated in cyber security and reliable security solutions.
24. You or the business pays attention to privacy policies of websites and before installing new software.
25. You or the business have passwords that are complex and not easily guessable.
26. Financial information about yourself, the business, employer or family is never disclosed online.
27. You or the business tailor access to your ICT reducing the risk of an internal breach.
28. You or the business knows if your bank uses fraud prevention systems that call out unusual purchasing behavior.
29. You or the business knows how to report hacking, stolen finances or identities promptly.
30. You or the business have an internet usage policy or agreement that clarifies what websites and web services you, employees and loved ones can use.
31. You or the business have a plan if you suffer a data breach or loss of personal, family, customer or employee information.
32. You or the business informs loved ones, customers or partners/suppliers on how to protect their personal and financial information.
33. You or the business keeps up with the increasing adoption of mobile and social media platforms.
34. You or the business have guidelines for yourself, employees and/or loved one's use of social media and social networking sites.
35. You or the business are prepared for and safe from *"Social Engineering"* attacks.
36. You or the business keeps up with news on mobile device security vulnerabilities.
37. You or the business use *"Multifactor Authentication"* to access networks.
38. You or the business completely wipes data off your ICT before disposing them.
39. You or the business discourages the use of USB devices at home and/or at the workplace.
40. You or the business shut off your ICT when not using them.
41. You or the business checks your credit statements monthly for any fraudulent activity from online transactions.
42. You or the business checks for new cybercrime protection products and services.
43. You or the business have passwords with more than five characters.
44. You or the business use different passwords at each website, service provider and banking account.
45. You or the business keeps your ICT current with the latest patches and updates.
46. You or the business always looks for the "locked" icon at commerce sites.

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)

47. You or the business regularly makes sure your ICT is configured securely.
48. You or the business never responds to email messages that ask for personal information.
49. You or the business are educated on the elements of *"Internet Fraud"*.
50. You or the business are aware that prompt and effective action is critical to protecting your digital & corporate reputation.
51. You or the business encrypt hard drives to help protect vital data in case of theft or loss.
52. You or the business uses a pass code on mobile phones and subscribe to a remote wipe service.
53. You or the business knows what personal and financial information you have on all internet enabled devices.
54. You or the business monitors who sends sensitive personal information from your home and/or business.
55. You or the business monitors how personal and financial information is disseminated online.
56. You or the business knows where you keep information collected at each entry point (i.e. central computer database, individual laptops, disks, cloud).
57. You or the business pays special attention to how and where you store personally identifying information.
58. You or the business delete, shred and destroy personal or customer credit card information unless it has a relevant or business need.
59. You or the business have a data security plan that includes physical security, electronic security, employee training, and the security practices of contractors and service providers.
60. You or the business can identify the computers or servers where sensitive personal information is stored.
61. You or the business can identify all connections to the computers where you store sensitive information.
62. You or the business regularly assesses the vulnerability of social media profiles to known or foreseeable attacks.
63. You or the business ensures you do not store sensitive financial or consumer data on any internet enabled device unless it is essential.
64. You or the business regularly checks expert websites and your software vendors' websites for alerts about new vulnerabilities.
65. You or the business scans the ICT on your network to identify and profile the operating system and open network services.
66. You or the business transmits credit card information or other sensitive financial data using Secure Sockets Layer (SSL).

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)

67. You or the business use password activated screen savers to lock computers after a period of inactivity.
68. You or the business locks out users who do not enter their correct password within a designated number of log-on attempts.
69. You or the business at once changes vendor-supplied default passwords when installing new software.
70. You or the business restricts the use of ICT to those who need them to perform their jobs or academics.
71. You or the business store your ICT in a secure place.
72. You or the business knows who to notify if there is a security breach.
73. You or the business investigates security incidents in a proactive manner and take steps to close off existing vulnerabilities.
74. You or the business password protects all mobile devices that hold sensitive data and encrypt them.
75. You or the business securely back up mobile devices often.
76. You or the business rarely misplaces portable electronic devices.
77. You or the business turns off wireless services when they are not being used.
78. You or the business keeps your mobile device security software current by having the latest mobile security software, web browsers and operating systems.
79. You or the business review the privacy policy and understand what data (i.e. location, access to your social networks) on mobile devices an application can access.
80. You or the business knows how to disable the geotagging feature on mobile phones.
81. You or the business knows about Wi-Fi hotspots and types of financial and business functions to limit.
82. You or the business knows when banking and/or shopping to look for web addresses with "https://".
83. You or the business are familiar and protected from credit card fraud.
84. You or the business are familiar and protected from identity theft.
85. You or the business are familiar with DHL/UPS scams.
86. You or the business are familiar with Escrow Services Fraud.
87. You or the business are familiar with Internet Extortion.
88. You or the business always figures out the minimal amount of information you must give online.
89. You or the business contacts the seller with questions before bidding on auction sites like eBay.
90. You or the business are cautious when dealing with individuals outside of your own country.
91. You or the business makes sure a website is secure and reputable before giving a credit card number.

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)

92. You or the business have never given credit card information through unsolicited emails.
93. You or the business know to contact the Better Business Bureau to decide the legitimacy of a company.
94. You or the business are wary of businesses that operate from P.O. boxes or mail drops.
95. You or the business keystroke in a website domain rather than clicking on a link provided in an email or attachment.
96. You or the business are cautious when a site requests payment to an *"agent",* instead of a corporate entity.
97. You or the business ensure websites are secure prior to giving a credit card number.
98. You or the business reports unauthorized transactions to your bank or credit card company as soon as possible.
99. You or the business use the most up-to-date patches for your software.
100. You or the business never assumes a company is legitimate based on the "appearance" of their website.

Yes Answers__ No Answers__ I Do Not Know__ Does Not Apply__

Yes Answers__ + Does Not Apply__ = CCPC Score__

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

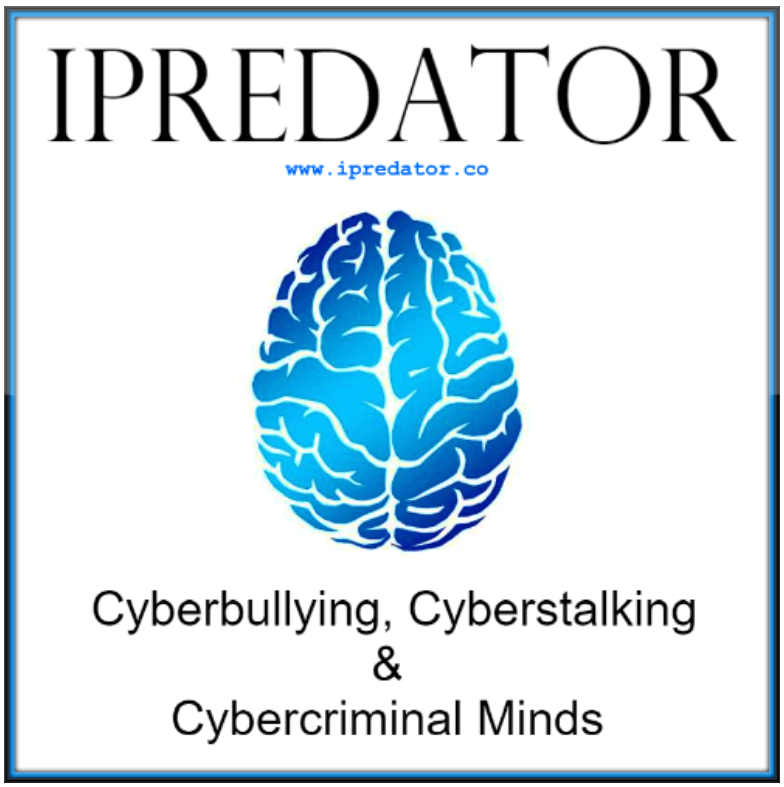
Note: The goal for optimal internet safety & cyber security functioning is to score a 90 or higher. *"I Do Not Know"* & *"No"* responses should be addressed at once with a plan of action.

(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 CCPC 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

Cybercrime Protection Checklist
CCPC

Note: Just as all the IISC tools, it is recommended to take the CCPC 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 Cybercrime 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 Cybercrime 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 Cybercrime 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 Cybercrime 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 Cybercrime 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 Cybercrime 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 Cybercrime 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.