IROC2.ORG
Public and Permanent™

The History and Rationale Behind The Digital Risk Assessment

The Digital Risk Assessment is a popular tool created by the Institute for Responsible Online and Cell-Phone Communication to help make the line between responsible use and abuse clear. The assessment was conceptualized based on the increased momentum of society's narcissism and voyeurism, as if they were two speeding locomotives headed towards each other until they collide, creating what looks a spike. The Assessment helps to illustrate how much negative attention you are calling to yourself based on your digital behaviors, and the likelihood of suffering a negative consequence as a result of your digital behaviors. It consists of a series of questions that helps to cast a light on the poor judgment you may be unknowingly, or blindly, employing with digital tools and technologies so you can stop immediately.

The questions are very simple. All you have to answer are a series of "yes or no" questions. Depending on your answer, a point value is assigned and your "risk spike" is determined. The higher your risk spike, the more negative attention you are calling to yourself and your actions ─ the further you are from the line of digital consciousness. The more negative attention you call, the more temptation there is for "someone" to look in on you through your digital device, your "window to the world." Remember, your "window" works two ways, and all you have to do is give someone a reason to look in, and they will. However, if you stay close to the line of consciousness through responsible use, your odds of becoming a victim of a cyber-crime or digital exploitation are very low as you are only one in a billion digital users.

While the Risk Assessment was conceptualized from society's increase in narcissism and voyeurism, its actual creation and execution stems from an idea far more simple. Imagine you and I are standing outside of a stadium after a sporting event, just minding our own business. There are 50,000 people standing around us, and one of them is a pickpocket (a thief). If nobody in the crowd is doing anything to call attention to themselves, it is likely that the person who gets pick pocketed would have been selected at random by the criminal. Now imagine the same situation; however, just prior to the thief pick pocketing somebody, you stand up on a table in that sea of 50,000 people and hold up a sign with your full name, social security number, address, credit card number, bank card and pin and a sexy picture.

Whereas before you were just one person in a sea of 50,000 people who might get robbed, you have now just increased your chances of facing an issue (it is not guaranteed) because, you stood up and shared all kinds of personal information with complete strangers. In fact, with that kind of information, perhaps some people in the crowd who were not thieves before will be tempted to become one considering the information you just handed to them. By standing up and sharing certain information with 50,000 people, you increased your risk of exploitation.

The Risk Assessment applies the same theory. The more you answer yes, the more information you are sharing with the global [digital] village and everyone that lives in it. The more you answer yes, the higher you are holding a bull's-eye up over your head, and the larger the bulls-eye gets. However, if your answers are consistently "no" then your spike is low, thus you remain close to the line of consciousness. The lower your risk spike, the less negative attention you call to yourself, the less you stand out to everyone in the digital world, and the less liability you incur.

In Short, this assessment:

- is a series of questions that will help illustrate an individual's digital responsibility and assess their level of digital responsibility.
- Is a tool to help individuals reduce the risk of becoming a victim of harassment, cyberbullying, digital exploitation or social media assault by learning how and why it is important to self-monitor their own actions.
- offers insight into many different irresponsible behaviors and trends, and communicates the potential consequences of those actions while concurrently rewarding positive behaviors.

Taking the Digital Risk Assessment

Instructions:

1. Respond HONESTLY to each of the questions.
2. Once you have responded to all statements, review your point total.
3. Apply your score to the Assessment Key to gauge your use / abuse of digital tools & technology.

Important Notes:

1. Entering personal information on a secure (https) site for purchases, banking, etc does NOT apply here.
2. A picture, video, or text you would not show family or an enemy does NOT mean it has to be sexual in nature.

Digital Risk Assessment: Questions

1. I have a **PERSONAL** social web page (e.g. Facebook, My Space, Linked In, Blogger, etc).

   ❑ **YES** ❑ **NO**

2. I have posted my **PERSONAL** phone / cell number on a social website, chat room, board, etc.

   ❑ **YES** ❑ **NO**

3. I have posted my **HOME** address on a social website, chat room, public board, etc.

   ❑ **YES** ❑ **NO**

4. I have posted my **SCHOOL / WORK** address on a social website, chat room, public board, etc

   ❑ **YES** ❑ **NO**

5. I post current / future status updates - Example: Going on vacation tomorrow.

   ❑ **YES** ❑ **NO**

6. I think deleting a file (pic, vid, text, etc) from Digital Tools removes it permanently.

   ❑ **YES** ❑ **NO**

7. I have anti-virus **AND** anti-spyware programs installed on my computer.

   ❑ **YES** ❑ **NO**

8. I run my anti-virus **AND** anti-spyware programs daily.

   ❑ **YES** ❑ **NO**

9. I believe that I am truly anonymous in a digital world.

❑ **YES** ❑ **NO**

10. I believe my social site (i.e. Facebook) password truly keeps my content private.

❑ **YES** ❑ **NO**

11. I have taken digital pics / vids of myself that I wouldn't show my family or enemy.

❑ **YES** ❑ **NO**

12. I shared pics, vids or text about myself I wouldn't show my family or enemy.

❑ **YES** ❑ **NO**

13. I do and say things in front of my webcam that I wouldn't show my family.

❑ **YES** ❑ **NO**

14. I have harassed or bullied others through digital technology.

❑ **YES** ❑ **NO**

SCORING:

1.	Yes - 10 Points
2.	Yes - 10 Points
3.	Yes - 10 Points
4.	Yes - 10 Points
5.	Yes - 10 Points
6.	Yes - 10 Points
7.	No - 20 Points
8.	No - 20 Points
9.	Yes - 20 Points
10.	Yes - 20 Points
11.	Yes - 50 Points
12.	Yes - 50 Points
13.	Yes - 100 Points
14.	Yes - 100 Points

The Digital Risk Assessment Key:

Below 30: As we become more dependent on digital technologies for both personal and professional purposes, it is virtually impossible for any of us to earn or maintain a score total of 0. The fact that you fall into this category means you are ahead of the game and do seem to be using your digital tools and technologies responsibly. By maintaining a score under 30, you reduce the chances that you will find yourself at the epicenter of a devastating digital issue or digital disease. If you are near a 30, see what you can do to realistically bring the number down as you are largely still in control of your digital content.

40 - 120: If your Risk Spike is this high, you are at moderate to high risk of facing a digital issue like identity theft or exploitation. A risk spike this high means that your personal information, schedule, lifestyle and identity is way too easy to find and exploit. If you fall into 80 or lower, you should immediately look at what items in the assessment you can reasonably stop doing ASAP to try and bring your score down. If you are over 80 and have not yet been affected, we suggest you start working to bring down your score ASAP. You may also want to start researching all email addresses and user names you have ever used online, as well as review search engine results for your real name. Finally, you may want to take a close look at your credit score.

130+: If your Risk Spike is 130+, we HIGHLY recommend you discuss your results with an authority figure and / or consult a cyber-safety professional. If your score is 130 or higher you are at high risk to face a severe and dangerous situation. The reason for the high risk alert here is that a score this high usually means that another person(s), besides you, is already in possession of private information and/ or content that can be used to harm or exploit you. They are in control of this content - not you - and whether they intentionally (e.g. for revenge) or unintentionally (e.g. lose their device) leak your digital content / information, you will have no power or recourse to get it back / offline.

A digital version of the risk assessment is available online at www.iroc2.org/CyberSafetyRiskAssessment.html