# Who is a cybersecurity professional?

Here, we come in with many unrefined industry practice assumptions, especially those new to the cybersecurity profession. Aspects such as hacking, scripting attacks, penetration testing, vulnerability assessment, social engineering, etc., can be very blurred to a non-experienced person despite being in the technology sector for a long-time. Personally, I have found the security speak quite boring and overly pessimistic to draw my interest in the past. However, I suppose I am on a transition journey to the enlightened side of the security revolution.

Regardless of my personal bias of cybersecurity as an overhyped technical elite phenomenon, it has become hard to ignore its daily carnage in every sector of our society. Hence, I have taken note, and I believe everyone should notice and play their part. For, I am convinced that cybersecurity is more than a technology issue. In fact, I would say it is a social construct aided by technology. Thus, access to technological tools to perform cyber exploits such as hacking for good, fun or evil (Black/grey/white hat hacker) unfortunately misses the mark by a longshot.

To become valuable ‘cyber hackers and operators,’ we need to take a multidimensional approach to cybersecurity. In which, firstly, we need to appreciate and understand our unwritten social contract with the fellow citizenry of the world. We all have a duty to social ethics and human rights. Secondly, and of course equally important, we need not be [script kiddies](https://www.wikihow.com/Avoid-Becoming-a-Script-Kiddie). We must be professional and polished at what we do by learning and gaining the necessary technical skills to serve and lead with excellence in the industry. Learning programming basics is undoubtedly the beginning of a successful cybersecurity career. Thirdly, we will need a lot of patience, commitment, good instinct and integrity. We must not fall for the easy or path of least resistance; when we have done our due diligence, and our instinct is clear. Then we must professionally call things as they are, regardless of other people’s entrenched interests.

With this approach, as cybersecurity professionals, we should do so with credibility and trust whenever we serve or lead in society. Scripting/programming, hacking, penetration testing, digital forensics, cybercrime, law and ethics, privacy and many more are all facets of cybersecurity we must warm up to as cybersecurity professionals without being shackled to a market tool or technology construct.

Ref:

Hacker-Roadmap <https://github.com/sundowndev/hacker-roadmap#difference-between-hacking-and-ethical-hacking>

Script kiddies <https://www.wikihow.com/Avoid-Becoming-a-Script-Kiddie>

Penetration Testing - Quick Guide: https://www.tutorialspoint.com/penetration\_testing/penetration\_testing\_quick\_guide.htm

Regards,

Andrew