As an attack vector social engineering has been utilised in many different crime areas and cybercrime is no exception. In fact, many internet security companies continuously highlight the human factor as the weakest link in cyber security. Influencing people into acting against their own interest or the interest of an organisation is often a simpler solution than resorting to malware or hacking.

Both law enforcement and the financial industry indicate that social engineering continues to enable attackers who lack the technical skills, motivation to use them or the resources to purchase or hire them. Additionally, targeted social engineering allows those technically gifted to orchestrate blended attacks bypassing both human and hardware or software lines of defence.