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.
EUROPOL PUBLISHES LAW ENFORCEMENT AND INDUSTRY REPORT ON SPEAR PHISHING

MAKING THE VOICES OF YOUTH ADVOCATES HEARD AT EUROPOL'S 1ST EUROPEAN YOUTH DAY

CLICK HERE AND SEE HOW YOUR MONEY DISAPPEARS – CRIMINAL #CYBERSCAMS OF THE 21ST CENTURY

INTERPOL-EUROPOL CONFERENCE CALLS FOR GLOBAL RESPONSE TO CYBERCRIME

15 WAYS YOU COULD BE THE NEXT VICTIM OF CYBERCRIME

EUR 8 MILLION, 700 BANK ACCOUNTS AND MONEY MULES: THE LITTLE-KNOWN TRICKS OF SOCIAL ENGINEERING FRAUDSTERS

EUROPOL REVIEW 2016 - 2017
Source URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/social-engineering