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.

NUMBER OF ITEMS FOUND: 31

SEARCH

TYPE

Article/Story, Event, How-To Guide, Landing Page, Multimedia, News/Press Release, Operation, Page, Publication/Document

TARGET GROUP

SEARCH

CLEAR ALL

27 Sep 2016

THE RELENTLESS GROWTH OF CYBERCRIME

NEWS/PRESS RELEASE

EUROPEAN CYBERCRIME CENTRE - EC3

TRAINING AND CAPACITY BUILDING

30 Sep 2015

3RD EUROPOL-INTERPOL CYBERCRIME CONFERENCE

EVENT

CRIME PREVENTION ADVICE-KNOW THE ENEMY!

HOW-TO GUIDE

24 Sep 2013

EUROPOL-INTERPOL CYBERCRIME CONFERENCE 2013

EVENT

21 Jan 2013

OFFICIAL LAUNCH OF THE NEW EUROPEAN CYBERCRIME CENTRE (EC3) CEREMONY

EVENT

« FIRST ‹ PREVIOUS 1 2 3

Source URL: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/social-engineering?page=2