Call for Chapters
The Routledge International Handbook of Social Engineering and Crime

Editor: Stephan G. Humer
Publisher: Routledge
Expected publication: 2028

Chapter proposals are invited for *The Routledge International Handbook of Social Engineering and Crime*, an interdisciplinary reference work that offers an accessible and comprehensive overview of Social Engineering as a crime phenomenon.

Social Engineering, often described as the “art of human hacking,” refers to the deliberate manipulation of people in order to obtain information, access, money, or compliance. Although cybercrime is often framed as a technical problem, many successful attacks rely less on code than on communication, trust, deception, pressure, routine, and situational ambiguity. This handbook addresses Social Engineering as a socio-technical and criminological phenomenon, showing how attacks are designed, how victims interpret and respond to cues, and how organizations and institutions seek to prevent, investigate, and govern such practices.

The volume brings together three perspectives that are too often discussed separately: first, the social and psychological mechanisms of manipulation, including authority, urgency, reciprocity, social proof, and cognitive shortcuts; second, socio-technical attack practices across analog, digital, and hybrid settings, ranging from impersonation and pretexting to phishing, vishing, smishing, and AI-enabled deception; and third, criminological, legal, and justice-oriented perspectives on prevention, investigation, evidence, regulation, and governance.

Rather than focusing on a single domain such as IT security, psychology, or law, the handbook examines Social Engineering holistically: how offenders identify targets, construct plausible narratives, exploit organizational routines, and adapt to resistance; how individuals and groups make decisions under uncertainty; and how institutions respond through awareness measures, process controls, incident response, reporting structures, and legal remedies. Case-based chapters are particularly welcome, as they can illuminate recurring tactics, vulnerabilities, and institutional challenges across sectors and contexts.

The volume also looks ahead by examining how AI technologies—especially AI-generated media, deepfakes, and voice cloning—may transform manipulation at scale and reshape both opportunities for offenders and challenges for prevention, attribution, and justice.

Contributions from scholars and practitioners in criminology, sociology, psychology, media and communication studies, law, cybersecurity, information systems, policing, fraud prevention, intelligence, and related fields are welcome.

Structure of the volume

Part I: Social Engineering History and Theory
This part brings together chapters on the conceptual foundations of Social Engineering, the historical antecedents of deception, confidence tricks, and manipulation, the relationship between fraud, persuasion, and trust, and theoretical approaches from criminology, sociology, psychology, and science and technology studies.

Part II: Psychological and Sociological Methodology
Contributions to this part may address psychological mechanisms of influence and compliance, cognitive biases and heuristics, situational decision-making under stress and uncertainty, social roles, norms, and interaction order, organizational culture and vulnerability, as well as methodological approaches for studying manipulation, deception, and attack processes.

Part III: Social Engineering and Criminology
This part focuses on offender rationalities and scripts, victimization and repeat victimization, routine activity and opportunity structures, fraud ecosystems, policing and investigation, evidence and attribution problems, reporting and underreporting, legal frameworks, and questions of governance, regulation, and institutional accountability. This part also welcomes contributions on awareness training, security education, and organizational prevention strategies aimed at strengthening resilience against social engineering attacks.

Part IV: Classic Case Studies: Social Engineering
Relevant chapters may examine impostor scams, confidence tricks, insider elicitation, physical intrusion through deception, pretexting, fraud by telephone or face-to-face interaction, and historically important or paradigmatic cases that reveal enduring mechanisms of manipulation.

Part V: Modern Case Studies: Social Hacking
This part welcomes case-based contributions on phishing, spear phishing, vishing, smishing, business email compromise, romance fraud, social media-enabled manipulation, hybrid online-offline attack chains, attacks on public institutions and critical infrastructure, and sector-specific cases in finance, health, education, government, and business.

Part VI: Future Perspectives on Social Engineering
Future-oriented chapters may explore AI-generated persuasive content, synthetic identities, deepfakes, voice cloning, automated scam operations, platform governance, detection and defense, digital literacy, institutional resilience, and future research agendas, methods, and tools.

Desired contributions

Proposals for original chapters are invited. Contributions should be clearly written, empirically grounded, and accessible to an interdisciplinary readership. Contributions may be conceptual, empirical, comparative, methodological, legal, policy-oriented, or case-based. Chapters that connect different perspectives, for example, psychological mechanisms with organizational vulnerabilities or case studies with criminological theory, are especially encouraged. Authors are encouraged to write in a style suitable for a handbook: informative, synthetic, and accessible, with a clear argument and strong relevance for readers from different disciplinary and professional backgrounds.

Submission procedure

Please submit a chapter proposal including:

- a proposed chapter title
- an abstract of approximately 300–500 words

- 5–7 keywords
- a short author biography of approximately 100–150 words
- full contact details and institutional affiliation

Please send proposals to: stephan@humer.de

Important dates

Proposal submission deadline:	May 31, 2026
Notification of acceptance:	June 30, 2026
First full chapter submission:	February 28, 2027
Editorial review and feedback:	May to August 2027
Revised chapter submission:	September 30, 2027

Chapter length and format

Accepted chapters should normally be between 6,000–12,000 words, including references. Formatting and style guidelines will be provided upon acceptance.

Proposals that help develop a comprehensive and forward-looking understanding of Social Engineering and crime across disciplines, sectors, and contexts are particularly welcome.

For questions, please contact:

Professor Dr. Stephan G. Humer

Fresenius University of Applied Sciences Berlin
Brandenburg University of Applied Sciences (humer@th-brandenburg.de)

Please send proposals to: stephan@humer.de