Social Engineering Code of Ethics

The Social Engineering Code of Ethics accomplishes three important goals:

- It promotes professionalism in the industry,
- It establishes ethics and policies that dictate how to be a professional SE, and
- It provides guidance on how to conduct a social engineering business.

Chris Hadnagy, CEO of Social-Engineer, LLC has a motto, "Leave them feeling better for having met you." This motto developed into a core company value that resonates throughout the code of ethics that Chris designed. The following 11 bulleted points comprise the **Social Engineering Code of Ethics:**

- Respect the public by accepting responsibility and ownership over your actions, and their effects on the welfare of those in, around, and involved with the engagement.
- Before undertaking any social engineering engagement, ensure you are fully aware of the scope and effects on others and their well-being.
- Avoid engaging in, or being a party to, unethical, unlawful, or illegal acts that negatively affect your professional reputation, the information security discipline, the practice of social engineering, others' well-being, or the parties and individuals in, around, and involved with the engagement.
- Reject any engagement, or aspect of an engagement, that may make a target feel vulnerable or discriminated against. This includes, but is not limited to, sexual harassment, offensive comments (verbal, written, or otherwise) related to gender, sexual orientation, race, religion, or disability; stalking or following, deliberate intimidation, or harassing materials. Additionally, lewd or offensive behavior or language, which may be sexually explicit or offensive in nature, materials or conduct, language, behavior, or content that contains profanity, obscene gestures, or gendered, religious, ethnic, or racial, slurs are all to be avoided. Employing any of these tactics reduces the target's ability to learn and improve from the engagement.
- Do not negatively manipulate, threaten, or make others uncomfortable in any way, unless specified by a client due to unique needs and testing environment.
- Minimize risks to the confidentiality, integrity, or availability of information of your employer, clients, and individuals involved in engagements. After performing a social engineering engagement, ensure the security of obtained information is a priority. Never disclose information to outside parties as private and confidential

information must remain private and confidential. Do not misuse any information or privileges you are afforded as part of your responsibilities.

- When training future social engineers, consider that training will leave a lasting impact on your students and the methodology with which you train will echo through all students' future engagements. Provide students with the knowledge and tools to create positive learning environments and productive scenarios for their future engagements and clients.

- Ensure the social engineering practices of yourself and your students include conscientious, thoughtful, and considerate ways to escalate engagements to eventually emulate real-world attack vectors. Recognize our clients are seeking ways to improve their security posture and work with them to increase the difficulty of realistic attack vectors.

- Respect that social engineering engagements involve human vulnerability and avoid publicizing vulnerabilities, whether through a blog, social media, or other medium, that result in harmful effects, emotions, or feelings for your client and the individuals and parties in, around, and involved with the engagement.

- Do not misrepresent your abilities or your work to the community, your employer, or your peers. Ensure you have the experience and knowledge promised to your clients and stakeholders.

- Leave others feeling better for having met you.

If you have any questions, please email contact@humanhackingconference.com.