Security Awareness Training for
Social Engineering

Hacking Humans

Do your employees know how to NOT be exploited?

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Smooth talkers; simple curiosity gimmicks such as email birthday cards; urgent need requests and calls from fictional VIPs; auditors; system repair calls; friend requests on social media, fictional email threads, spam, malware; leaks; insiders; …. the ways of gaining access are infinite. And the ways of gaining access are getting pretty unique.

Human vulnerability cannot be patched, only prevented.

We cover:

- Types of Social Engineering
- Behaviors vulnerable to attack
- Social Engineering Threats and Defenses
- Countermeasures for Social engineering
- Policies and Procedures
- Identity Theft
- Countermeasures for Identity theft

Find us at procysive.com

Procysive

ANDREWS INTERNATIONAL