“**Social Engineering:** 'Banking' On Your Organization's Weakest Point—The Employee”

Pat Wilbur

Department of Mathematics and Computer Science,
Clarkson University

Social Engineering?

"**Social engineering** is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access..."

– Source: Wikipedia

Goal of Social Engineering

To trick an individual or members of an organization into performing a particular action, or letting an unauthorized individual sufficient access for performing that action, which is usually of some personal benefit to the unauthorized individual.

Perspectives on Social Engineering

Social Engineering as Lying:

- Social engineers outright disguise their identities and intentions during an attack
- Social engineering can be much more complicated than simple lying, often requiring extensive research and probing of the operation, management, and policies of an organization.

Perspectives on Social Engineering

Social Engineering as Confidence Trickery:

- In social engineering, members of an organization are misled in many ways similar to victims of a confidence trick (or “con”).
- Both social engineering and confidence tricks are often performed with the intent of financial gain, knowledge, or other personal gain.

Perspectives on Social Engineering

Social Engineering as Fraud:

- Criminal law identifies deliberate misrepresentation for personal gain as a crime.
- Such misrepresentations also violate civil law.
- Fraud encompasses deceiving with the intent to property, services, or information unjustly.

Common Techniques

Pretexting

Gimmes

Phishing

Quid pro quo

Exploiting Cognitive Biases

"IS FUN."

–Anonymous

Exploiting Cognitive Biases

"IS A GREAT WAY TO GET WHAT YOU WANT!"

–Anonymous

Exploiting Cognitive Biases

"Is generally mean and probably illegal."

–Me

Exploiting Cognitive Biases

People tend to trust the intentions of those who sound or look like officials.

People tend to believe stereotypes.

People tend to trust those who are handsome, modest, and seem naturally a little friendly.

Areas of Risk

Phone

Building Entrance

Office

Mail Room

Equipment / Phone Closet

Dumpsters

Internet / Intranet

Combat Strategies

Training, Training, and Training

Tight Badge Security + Security Officers

Require Escorts for All Guests

Lock & Monitor Mail Room and Equipment Closets

Restrict / Trace Overseas & Long-Distance Calls

Combat Strategies

Shred Important (or All) Trash, Erase / Shred Media

Awareness of System and Network Changes

Mark and Lockup “Confidential” Documents

Assign Employee PINs for Helpdesk Calls

Attractive Targets

Financial Institutions

Government Agencies

Other Big Business

Real World Examples