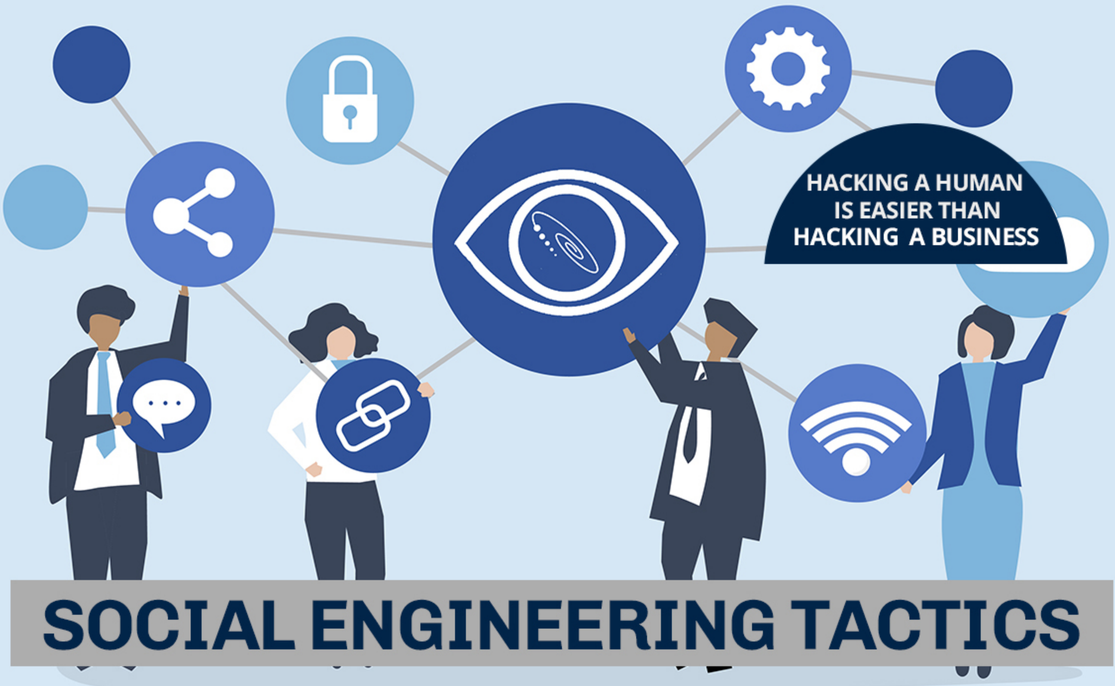
YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS




# SOCIAL ENGINEERING TACTICS

## 3 BASIC TYPES OF SOCIAL ENGINEERING TACTICS


## IN-PERSON SOCIAL ENGINEERING TACTICS

THE MOST COMMON TACTICS USED TO GAIN ACCESS, GATHER SECURE INFORMATION AND PLANT DEVICES YOU SHOULD KNOW:

**OPEN ACCESS -** When someone uses or requests to use your computer for whatever reason and they're left unmonitored. This often comes as a troubleshooting request for support.

**OPEN DOOR -** When you leave your door open at your company and someone slipd through.

**ROGUE EMPLOYEE -** When a maliciouos employee is hired with the purpose of gaining on-site access.

**THE CABLE GUY-** When someone pretends to be a service technician of some kind (DSTV, phone, electrician, etc.) to gain access to your business.

**BAR HOPPING -** When someone buys you drinks to extract information from you as you get drunk. Some people tend to do more talking when drinking.

**DEVICE LEAVE BEHIND -** When someone leaves behind a device laying around that tempts others to plug-in and open. Like a music CD, flash drive, or another common storage device.

**SIX DEGREES OF SEPARATION -** When someone learns about about your social practices and uses social relationships to gain your trust.

**NEAURO-LINGUISTIC PROGRAMMING -** When someone mirrors body language, voice and vocabulary to build a connection on a subconcious level. Usually touchy-feely.

## THE GOOD NEWS

THERE ARE FACTORS THAT CAN DECREASE THE PROBABILITY OF A SOCIAL ENGINEERING ATTACK

- Employee Training
- Extensive Use of Encryption
- Control Employee Access to Data
- Create BYOD Policies
- Implement Firewall Security

**68%**
of small businesses store customers' email addresses unsafely
(Small Business Trends)

LANDYNAMIX
Creating Value Through Technology Enablement

To get more information on these social engineering tactics visit:

https://landynamix.co.za/what-is-social-engineering.html


**References**

https://searchsecurity.techtarget.com/definition/social-engineering
https://www.social-engineer.org
https://www.digitalndigital.com/social-engineering-on-social-media/
https://en.wikipedia.org/wiki/Social_engineering_(security)
https://www.csoonline.com/article/2130996/cso-s-ultimate-guide-to-social-engineering.html