Physical Security Assessment

DISCRETE.
PERSONAL.
PROFESSIONAL.
EFFECTIVE.

Social Engineering

Social engineering is an uncomfortable subject, it's about people being "conned" whether for real of for testing purposes. When the Social Engineering is discovered and the target informed, the feeling of "shame" is high. They can feel like they have let themselves and the organisation down. We therefore strongly recommend Social Engineering (like phishing) is only done after some training and anyone caught out is very carefully told.

Social engineering is aimed at gaining cyber and/or physical access to restricted rooms and buildings for vulnerability assessment and security testing. Dressing formally can help someone gain access to offices and corridors, acquiring a maintenance uniform can help solidify access to server rooms and building facilities, and donning a hospital uniform can aid with access into healthcare facility terminals.

The Social Engineering Sting

Tailgating is popular technique to gain access to secured buildings. This simply involves following and entering a door opened by approved personnel. By assuming the 'identity', (not literally), of someone who is supposed to be there avoids suspicion. A similarly approaching the door with both hands/arms full of files, cakes or coffee, well timed, works equally well. People like to be polite.

With access to the building, the same techniques can be used for other rooms or restricted areas. An individual can pose as a technician bringing equipment to the server room. Any role or function can be used for this approach, usually for more mundane and predictable things. It may be a technician, a low-key employee, an official delegate, an IT specialist, or even a consultant.

> *We found a few gaps in our systems that needed covering as well as some industry insights that we hadn't thought of.*
>
> ***JOHN CARTER - Owner***
> ***AGS PRESIDENT***
> ***Jack Lewis Jewellers - IL***

Tailgating

Tailgating occurs when an unauthorized person slips in through a door before it closes and has the potential to expose your workplace to a variety of threats.

Theft

Allowing unauthorized individuals into secured areas can result in tangible losses to include:

- Office equipment
- Intellectual property
- Sensitive hardware
- Employee personal items such as phones, wallets, purses and other valuable items

Piggybacking

Piggybacking occurs when an authorized person allows someone to follow them through a door to secure area. Piggy backing is primarily a behavioural issue that circumvents established access control procedures

Working Environment

An unsecured environment that does not have access controls is more susceptible to:

- Workplace Violence
- Active Shooter
- Domestic Violence
- Acts of Terrorism

HMH Consultants

The team at ***HMH Consultants*** are experts at identifying conducting physical security reviews and social engineering, with many years' experience which gives the team the confidence to walk brazenly into office environments in someone else's persona. Reports are clear and easy to understand and if needed the team can assist with additional training and awareness campaigns.

Contact Us

+1 346 762 8653 (USA)
+44 (0) 7554445855 (UK)
info@hmhconsultants.com.com
https://hmhconsultants.com/

632 W Alabama St, Houston Tx, 77006, USA
Unit 7 Moston Court,
Weston Super Mare,