Threatlandscape

Access: Human Element

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

In this presentation we focus on how malicious actors gain access to information assets.

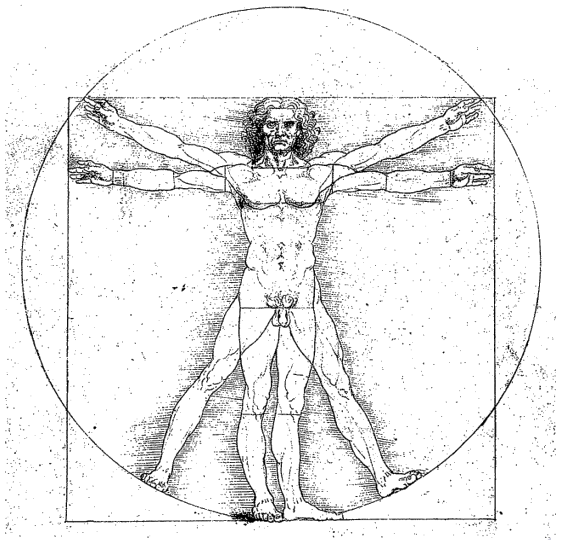
Big Question

How do they gain access?

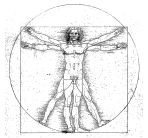
Big Question
How do they gain access?

According to DBIR 2021 report, 85% of the breaches involved some sort of human involvement. In this video we talk about social engineering, a way to exploit the human nature to gain access.

Human Element



Human Element



Installing anti-malware solutions, closing all the ports, using hard to guess passwords are all technical solutions that are increasing the security of your systems. Unfortunately, no matter how tight you lock systems down, it is all for naught if someone from the inside goes about opening those systems up.

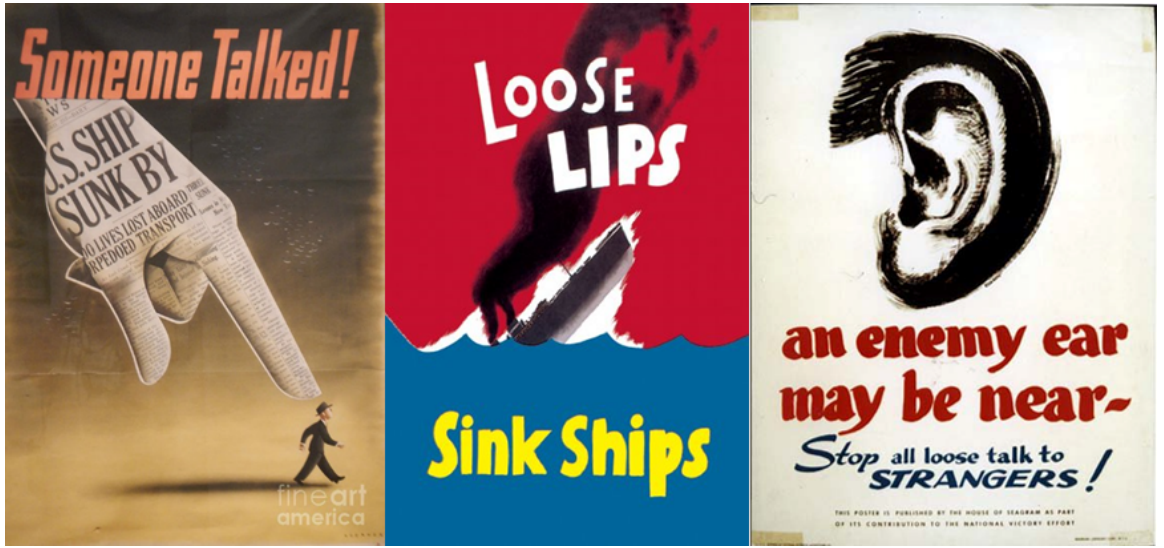
We are not necessarily talking about insiders here. People want to be helpful by their nature. Keeping a door open may seem like the polite thing to do but it is a known tactic to piggy back on other people to gain access to restricted areas.

Social Engineering

Social Engineering
WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES

Social engineering is the practice of exploiting human nature to gain access to information. Its proponents call it a forever day vulnerability.

What to Do?



What to Do?

As individuals we should be careful about what information we divulge. As organizations, we should make sure our employees are constantly reminded of security implications of their behavior. This is covered in awareness training.

Furthermore, the employees that have access to critical information and systems should receive training appropriate for their role.