Don't help the attacker – insider awareness lecture

Lecture length: 90 minutes

Lecture goals: For many years now, one of the leading ways for hackers to infiltrate an organization's computer systems and bypassing the various security measures set forth by the IT is by taking advantage of employees of the target organization. These are not necessarily malicious employees, but sometimes just indifferent or negligent. Remember, an attacker needs only one employee to break the rules in order to infiltrate the network and wrack havoc.

In this lecture we are going to cover basic and very advanced techniques employed by attackers, and most importantly we will see what we must and mustn't do in order to keep our critical infrastructure safe from harm.

Target audience: Each and every employee in the organization. No background in cyber, hacking or programming is needed.

Curriculum:

- Introduction
  - Who are our attackers & why are they after us
  - APT's and their capabilities – What can attackers do when they have money
  - Insider types (mainly careless insider)

- Passwords
  - The weakness of passwords
  - How are password stored
  - Attacking passwords (guessing, dictionary, reuse, brute-force, hash cracking)

- Physical security
  - The dangers of physical accesses by an attacker
  - The risks of BYOD
  - Various tools, capabilities and techniques employed by attackers

- Daily use & Development related risks
  - The risk of MITM in public WiFis
  - The risks of public code and files shares (such as Github or AWS buckets)
  - The risk of MITC
  - The world of 3rd party pain
  - The importance of automation in DevOps

- Summary
  - Don’t bypass cyber security rules and regulations
  - The security <-> usability balance
  - Never blindly trust passive solutions (AV, IDS, FW)
  - Bonus: Automation is a double edged sword (also used by attackers)

Good luck!