Social Engineering – How to Avoid Being a Victim

Social engineering (an act of exploiting people instead of computers) is one of the most dangerous tools in the hacker's toolkit to breach internet security. The Ubiquiti Networks fell victim to a $39.1 M fraud as one of its staff members was hit by a fraudulent "Business Email Compromise" attack. Thousands of grandmas and grandpas are victim of phishing emails and are forced to pay ransom to have their data released.

In this new millennium, the cyber security game has changed significantly from annoying harmless viruses to stealing vital personal data, causing negative financial impact, demanding ransom, and spreading international political feud. Anyone with presence in the Cyber space has to protect himself/herself, the infrastructure, customers, and also deal with the legal repercussions in the event of a breach. This mini-workshop presents the different types of social engineering practices including use of social networks such as Facebook, Twitter, LinkedIn, the bad guys successfully use. The victims can range from the "C" levels (CEO, CFO, CTO) down to the individual contributors in an organization to a grandparent on her laptop. The talk discusses a variety of ordinary but effective measures such as awareness campaign that organizations can take to minimize the risk of breach.