Phishing Awareness Lecture

Workshop length: One half-daily session (4 hours)

Workshop goals: For many years now, Email has been the #1 delivery vehicle for malware of all sorts (such as ransomware). Symantec, one of the world's leading security firms released a statistic that states that in 2016, **1 in 131 emails contained malware**. IBM researches have calculated that the rate of those emails grew by 4X times in that year, and that the rate just keeps growing.

Hackers don't just use Emails to spread their malware – over 400 businesses are attacked worldwide on every day using BEC schemes on which fake emails are sent to employees pretending to come from a manager in the organization and request immediate money transfer. This might sound easy to spot, but when giant companies such **Google and Facebook** who are well aware of cyber security fell victims to such attacks and **lost over 100M$,** we should all be concerned.

As these attacks happen on a daily basis, even here in Israel, this workshop is a must for each and every employee in every organization. In this workshop we will get familiar with common attack vectors and techniques hackers use to attack our employees via Email, phone and SMS messages. We will understand how to identify such fake messages, and gain tools to decide which message is risky and which is benign.

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

Curriculum:

- Who are those attackers
- Types of attacks (Ransomware, RAT, Adware, Spyware, Crypto-Miners, BEC)
- Social engineering that effects us all:
    - Phishing (Attacking via Emails)
    - Vishing (Attacking via Phone calls)
    - Smishing (Attacking via SMS messages)
- **Crucial tips for staying secure**

Good luck!