# Problem Domain

Current security processes and technologies have made progress in making it more difficult for malicious actors to break into the company’s cyber defenses. However, despite significant efforts and investments from organizations to improve their cybersecurity posture, we can say that there is still no such thing that will be 100% secure. As a consequence of improved security measures, these malicious actors are always looking for alternative ways to break into the company’s cyber defenses and have significantly increased the phishing attacks targeting what I call our last line of defense, the human. Simply put, no matter how much money and resources are poured into a company’s infrastructure for cyber defense, we’re only as secure as the weakest link. Susceptible employees have remained a major concern for companies more so nowadays because more than 90% of successful ransomware attacks is attributed to phishing attacks. While some companies have created an anti-phishing campaign for awareness, this is not enough. We need implement an effective and complete Phishing Defense Program. How do we do this?

# Introduction

What is phishing? Phishing is a type of social engineering where an attacker sends a fraudulent message normally in the form of email and is designed to trick a human victim into revealing sensitive information to the attacker, download and install malicious software on the victim's infrastructure like ransomware and send money or gift cards to the cybercriminal. Phishing attacks normally use emotions like fear, curiosity, urgency, and greed to trick susceptible recipients.

One can say that cybercriminals don’t break-in anymore, they login or just ask susceptible people to do their bidding. They do this by attacking target organizations with relentless phishing attacks hoping to victimize a susceptible human, tricking that human into clicking on a malicious link, downloading a malicious attachment, giving away user credentials or sending high value gift cards. And despite the best efforts in employing a defense-in-depth approach in protecting the organization, a lot of these phishing attacks still reach employee mailboxes.

In an effort to address this, organizations started creating and establishing a phishing awareness program, where they target employees with simulated phishing campaigns with the goal of educating them on what a phish is and how to identify it. But how do you effectively run a phishing awareness program? Is it by targeting all employees with the same phish? Do you think people in IT and Finance departments are susceptible to the same kind of phish? How about people in the Food Service and in Legal?

Do you think running a punitive phishing program will help where being susceptible multiple times can potentially lead to termination of employment?

Is running a phishing simulation enough? Or is this just one step towards creating a complete and effective phishing defense program?

We need to train employees to become human sensors and integrate them into the overall cyber defense program. If we are successful in doing this, we would have turned what I have described to be the weakest link in the cyber defense chain into one of our most valuable security assets.

The following questions should help us define how we can establish a complete and effective Phishing Defense Program.

1. How do we effectively train employees to become human sensors and be part of the overall cyber defense program?
2. How should employees behave if they suspect that they received a malicious email?
3. What ways can employees ask for assistance if they suspect that they received a malicious email?
4. How should IT support behave when employees report a potentially malicious email?
5. What ways can IT support respond to these reported potentially malicious emails?
6. If confirmed malicious, how can we implement some kind of prevention to prevent the same malicious email from reaching employee mailboxes?