# **Social Engineering Questionnaire**

The purpose of this document is to better understand the business, its environment, and how employees interact with the environment or with one another. The answers provided will help guide the direction of your phishing campaign.

1. What level of employee information will be provided to the campaign team? Would it include personal information such as first name, last name, payroll bank, etc.?
2. What common websites or applications do internal users utilize daily?
3. What are the most common file types users works with? (PDFS, Word, Excel, etc).
4. What organizations does the company work with? (Vendors, IT support, business partners, charities).
5. What is a major internal company product or service that employees prioritize the most?
6. Is there a group of employees who routinely fall for the Phishing emails?
7. Are there any blacklisted websites such as Gambling, Porn, etc. that employees are suspected to visit?
8. Is there segregation between the employees who handle sensitive information v/s employees handling public information? Do they use different systems?
9. How often is the security awareness training performed?
10. Do employees in different countries use different email domains and username format?
11. Is it a targeted Phishing campaign (i.e. Spear Phishing) or a generic Phishing campaign?
12. Are employees allowed to use social media sites such as Facebook, Twitter, etc. using their workstations and work emails?