**Логика сценария**

Помимо стандартного сценария с переходом на потенциально вредоносный ресурс существуют и другие варианты. Перечисляем некоторые из них:

- получение сотрудником фишингового письма, в письме ссылка на потенциально вредоносный ресурс, сотрудник переходит по ссылке, вводит в форму аутентификационные данные (такого рода сценарии как раз и были направлены)

- получение сотрудником фишингового письма со вложенным потенциально вредоносным файлом / ссылкой на сайт, с которого необходимо скачать потенциально вредоносный файл

- сотруднику приходит письмо от злоумышленника, в котором он просит в ответ отправить данные по сотруднику, например, IP адрес его компьютера, его аутентификационные данные, сертификат безопасности, или выполнить потенциально опасную команду в командной строке, установить определенный плагин

- вишинг – сотруднику звонит злоумышленник и просит его выполнить потенциально опасные действия: ввести какую-либо команду в командной строке, например, по смене пароля от его учетной записи, перейти на сайт, который он диктует, и оставить там свои аутентификационные данные / скачать потенциально вредоносный файл

- злоумышленник связывается с сотрудником по смс-сообщению / телеграм канал

**Ниже перечислены разные виды атак на сотрудников:**





 