PROGETTO S5L5

**Obiettivo del compito:** creare una simulazione di email di phishing usando ChatGpt.

**Scenario**: La piccola impresa di famiglia Macchinari S.r.l., specializzata nel noleggio di macchinari edili, decide di ampliarsi e si rivolge alla Banca Moderna per richiedere un mutuo.

**Scopo**: L'attaccante, analizzando il contesto di ingegneria sociale, viene a conoscenza di questa informazione e decide di sfruttarla a suo favore per rubare dati finanziari. Finge quindi di inviare un'email dalla banca a cui l'azienda si è rivolta, realizzando un attacco di phishing mirato a sottrarre denaro dal conto aziendale.

**Mail:**



Questo tipo di email, se analizzata attentamente, presenta i classici segnali di un attacco di phishing, come:

* **Richiesta urgente**: cerca di spingere il destinatario a prendere decisioni affrettate.
* **Richiesta di informazioni personali tramite QR code**: molto sospetta, poiché le banche non chiedono mai dati personali in questo modo.

È fondamentale analizzare il numero di telefono fornito e il link prima di inserire dati che potrebbero causare danni.

Un'email di questo tipo potrebbe ingannare il destinatario per diversi motivi:

* **Linguaggio formale**: l'uso di un linguaggio professionale può far sembrare l'email autentica, portando a pensare che provenga da fonti ufficiali.
* **Nome e ruolo**: la presenza di un nome e di un titolo, come “Responsabile del Servizio Clienti della Banca Moderna”, rende l'email più credibile.
* **Riferimento a una richiesta reale**: menzionare l'apertura di un mutuo con la stessa banca può far sembrare l'email legittima.
* **Uso del QR code**: questa pratica può apparire più sicura e quindi spingere l'utente a fidarsi.